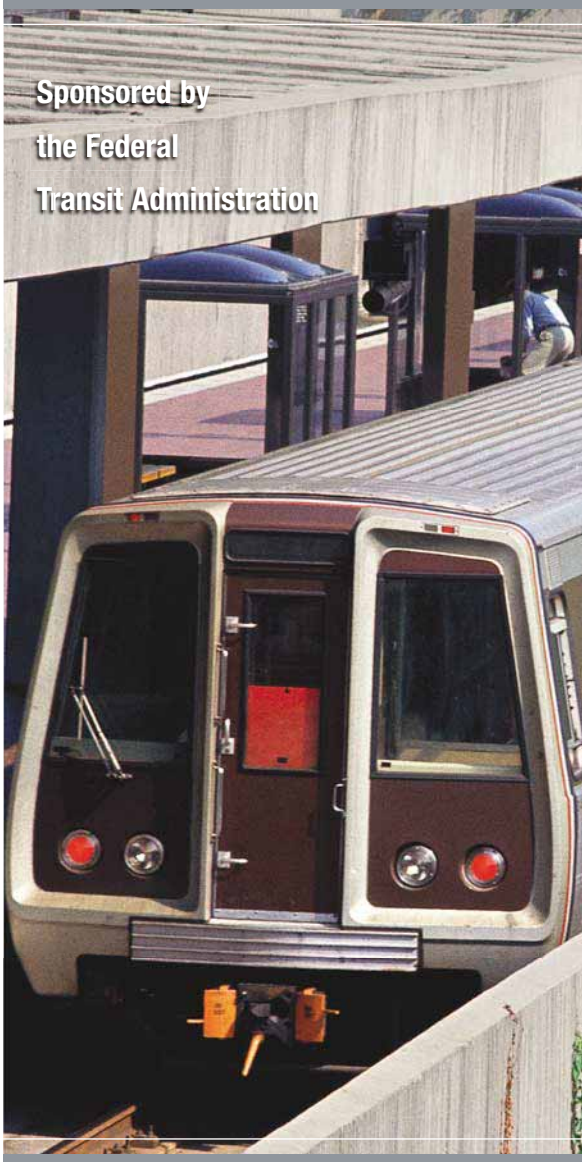
TCRP
REPORT 86

Public Transportation Security
Volume 4

Intrusion Detection for Public Transportation Facilities Handbook



TRANSPORTATION RESEARCH BOARD
OF THE NATIONAL ACADEMIES

TRANSIT COOPERATIVE RESEARCH PROGRAM

TCRP REPORT 86

Public Transportation Security:

Volume 4

Intrusion Detection for Public Transportation Facilities Handbook

SHAHED ROWSHAN
Science Applications International Corporation
Vienna, VA

and

RICHARD J. SIMONETTA
PBConsult
New York, NY

SUBJECT AREAS
Public Transit • Planning and Administration

Research Sponsored by the Federal Transit Administration in Cooperation with the Transit Development Corporation

TRANSPORTATION RESEARCH BOARD

WASHINGTON, D.C.
2003
www.TRB.org

TRANSIT COOPERATIVE RESEARCH PROGRAM

The nation's growth and the need to meet mobility, environmental, and energy objectives place demands on public transit systems. Current systems, some of which are old and in need of upgrading, must expand service area, increase service frequency, and improve efficiency to serve these demands. Research is necessary to solve operating problems, to adapt appropriate new technologies from other industries, and to introduce innovations into the transit industry. The Transit Cooperative Research Program (TCRP) serves as one of the principal means by which the transit industry can develop innovative near-term solutions to meet demands placed on it.

The need for TCRP was originally identified in *TRB Special Report 213—Research for Public Transit: New Directions,* published in 1987 and based on a study sponsored by the Urban Mass Transportation Administration—now the Federal Transit Administration (FTA). A report by the American Public Transportation Association (APTA), *Transportation 2000*, also recognized the need for local, problem-solving research. TCRP, modeled after the longstanding and successful National Cooperative Highway Research Program, undertakes research and other technical activities in response to the needs of transit service providers. The scope of TCRP includes a variety of transit research fields including planning, service configuration, equipment, facilities, operations, human resources, maintenance, policy, and administrative practices.

TCRP was established under FTA sponsorship in July 1992. Proposed by the U.S. Department of Transportation, TCRP was authorized as part of the Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA). On May 13, 1992, a memorandum agreement outlining TCRP operating procedures was executed by the three cooperating organizations: FTA, The National Academies, acting through the Transportation Research Board (TRB); and the Transit Development Corporation, Inc. (TDC), a nonprofit educational and research organization established by APTA. TDC is responsible for forming the independent governing board, designated as the TCRP Oversight and Project Selection (TOPS) Committee.

Research problem statements for TCRP are solicited periodically but may be submitted to TRB by anyone at any time. It is the responsibility of the TOPS Committee to formulate the research program by identifying the highest priority projects. As part of the evaluation, the TOPS Committee defines funding levels and expected products.

Once selected, each project is assigned to an expert panel, appointed by the Transportation Research Board. The panels prepare project statements (requests for proposals), select contractors, and provide technical guidance and counsel throughout the life of the project. The process for developing research problem statements and selecting research agencies has been used by TRB in managing cooperative research programs since 1962. As in other TRB activities, TCRP project panels serve voluntarily without compensation.

Because research cannot have the desired impact if products fail to reach the intended audience, special emphasis is placed on disseminating TCRP results to the intended end users of the research: transit agencies, service providers, and suppliers. TRB provides a series of research reports, syntheses of transit practice, and other supporting material developed by TCRP research. APTA will arrange for workshops, training aids, field visits, and other activities to ensure that results are implemented by urban and rural transit industry practitioners.

The TCRP provides a forum where transit agencies can cooperatively address common operational problems. The TCRP results support and complement other ongoing transit research and training programs.

TCRP REPORT 86: Volume 4

Project J-10A(3) FY'02
ISSN 1073-4872
ISBN 0-309-06760-X
Library of Congress Control Number 2002109708

Price $24.00

NOTICE

The project that is the subject of this report was a part of the Transit Cooperative Research Program conducted by the Transportation Research Board with the approval of the Governing Board of the National Research Council. Such approval reflects the Governing Board's judgment that the project concerned is appropriate with respect to both the purposes and resources of the National Research Council.

The members of the technical advisory panel selected to monitor this project and to review this report were chosen for recognized scholarly competence and with due consideration for the balance of disciplines appropriate to the project. The opinions and conclusions expressed or implied are those of the research agency that performed the research, and while they have been accepted as appropriate by the technical panel, they are not necessarily those of the Transportation Research Board, the National Research Council, the Transit Development Corporation, or the Federal Transit Administration of the U.S. Department of Transportation.

Each report is reviewed and accepted for publication by the technical panel according to procedures established and monitored by the Transportation Research Board Executive Committee and the Governing Board of the National Research Council.

To save time and money in disseminating the research findings, the report is essentially the original text as submitted by the research agency. This report has not been edited by TRB.

Special Notice

The Transportation Research Board of The National Academies, the National Research Council, the Transit Development Corporation, and the Federal Transit Administration (sponsor of the Transit Cooperative Research Program) do not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the clarity and completeness of the project reporting.

Published reports of the

TRANSIT COOPERATIVE RESEARCH PROGRAM

are available from:

Transportation Research Board
Business Office
500 Fifth Street, NW
Washington, DC 20001

and can be ordered through the Internet at
http://www.national-academies.org/trb/bookstore

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. On the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. William A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, on its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both the Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. William A. Wulf are chair and vice chair, respectively, of the National Research Council.

The **Transportation Research Board** is a division of the National Research Council, which serves the National Academy of Sciences and the National Academy of Engineering. The Board's mission is to promote innovation and progress in transportation through research. In an objective and interdisciplinary setting, the Board facilitates the sharing of information on transportation practice and policy by researchers and practitioners; stimulates research and offers research management services that promote technical excellence; provides expert advice on transportation policy and programs; and disseminates research results broadly and encourages their implementation. The Board's varied activities annually engage more than 4,000 engineers, scientists, and other transportation researchers and practitioners from the public and private sectors and academia, all of whom contribute their expertise in the public interest. The program is supported by state transportation departments, federal agencies including the component administrations of the U.S. Department of Transportation, and other organizations and individuals interested in the development of transportation. **www.TRB.org**

www.national-academies.org

AUTHOR ACKNOWLEDGMENTS

The *Intrusion Detection for Public Transportation Facilities Handbook* ("Handbook") is the result of the contributions from a number of individuals, transit authorities, and federal agencies. The Transit Cooperative Research Program (TCRP) funded the development of this Handbook, and the Federal Transit Administration (FTA) sponsored its preparation. The TCRP Project J-10A panel served as the primary advisor for this Handbook.

The information contained in the Handbook comes from the commercial state of practice for intrusion detection technologies with general and specific application to public transit agencies. The contribution of a number of metropolitan transit agency General Managers and representatives was critical in creating a document that reflects the needs of transit agency executives and managers for evaluating and upgrading intrusion detection technologies in public transit facilities.

The intrusion detection technologies introduced in this Handbook reflect the best judgment and experience of Science Applications International Corporation (SAIC) and PBConsult, who researched and developed this Handbook. The principal investigators of the project were Dr. Shahed Rowshan and Richard J. Simonetta. The other primary authors of this Handbook are Peter Michael, Charles T. Yengst, and Robert Brownstein. The contents of this Handbook were derived from personal interviews, literature reviews, transit site visits, and previous work in this area, but they do not represent an official view of any sponsor, transit administration, or federal agency.

FOREWORD

By S. A. Parker
Staff Officer
Transportation Research Board

This fourth volume of *TCRP Report 86: Public Transportation Security* will be of interest to general managers, senior executives, operational and technical managers, transit police, security personnel, and financial and procurement staff. Personnel with similar responsibilities at departments of transportation or public works will also find this report of value. The objective of this report is to address transit agencies' needs for evaluating and upgrading the intrusion detection systems applicable to the spectrum of their facilities (including tunnels, bridges, buildings, power stations, transfer stations, rail yards, bus yards, and parking lots) and their transit vehicles (such as buses, trains, support vehicles, and special purpose vehicles). The Handbook provides guidance on assessing system needs; developing system designs; and estimating system costs, benefits, and risks. The systems discussed in the Handbook range from low-technology to more complex high-technology systems and directly support the deterrence and detection of intrusion into secure areas. This volume was prepared by Science Applications International Corporation, under TCRP Project J-10A(3).

Emergencies arising from terrorist threats highlight the need for transportation managers to minimize the vulnerability of passengers, employees, and physical assets through incident prevention, preparedness, response, and recovery. Managers are seeking to reduce the chances that transportation vehicles and facilities will be targets or instruments of terrorist attacks and to be prepared to respond to and recover from such possibilities. By being prepared to respond to terrorism, each public transportation agency is simultaneously prepared to respond to natural disasters such as hurricanes, floods, and wildfires, as well as human-caused events such as hazardous materials spills and other incidents. In the last week of October 2001, the TCRP budgeted $2 million for security-related research in fiscal year 2002.

This is the fourth volume of *TCRP Report 86: Public Transportation Security*, a series in which relevant information is assembled into single, concise volumes, each pertaining to a specific security problem and closely related issues. These volumes focus on the concerns that transit agencies are addressing when developing programs in response to the terrorist attacks of September 11, 2001, and the anthrax attacks that followed. Future volumes of the report will be issued as they are completed.

To develop this volume in a comprehensive manner and to ensure inclusion of significant knowledge, available information was assembled from numerous sources, including a number of public transportation agencies. A topic panel of experts in the subject area was established to guide the researchers in organizing and evaluating the collected data and to review the final document.

This volume was prepared to meet an urgent need for information in this area. It records practices that were acceptable within the limitations of the knowledge avail-

able at the time of its preparation. Work in this area is proceeding swiftly, and readers are encouraged to be on the lookout for the most up-to-date information.

Volumes issued under *TCRP Report 86: Public Transportation Security* may be found on the TRB website at http://www4.trb.org/trb/crp.nsf/All+Projects/TCRP+J-10.

CONTENTS

EXECUTIVE SUMMARY

Prior to the attacks of September 11, 2001, many transit systems were already using a variety of intrusion detection strategies. Initially, these strategies were employed to reduce hazards, vandalism and crime; restrict access to secure areas; and raise passenger-perceived levels of security when using the transit system. The recent terrorist attacks and the threat of additional attacks have heightened security concerns, leading facility managers to deploy personnel to patrol or guard tunnels and other vulnerable areas.

The *Intrusion Detection for Public Transportation Facilities Handbook* ("Handbook") addresses transit agencies' needs for evaluating and upgrading the intrusion detection systems applicable to the spectrum of their facilities including tunnels, bridges, buildings, power stations, transfer stations, rail yards, bus yards, and parking lots, as well as transit vehicles such as buses, trains, support vehicles, and special purpose vehicles. The Handbook provides guidance on assessing system needs; developing system designs; and estimating system costs, benefits, and risks. The systems discussed in the Handbook range from low-technology to more complex high-technology systems, and directly support the deterrence and detection of intrusion into secure areas.

The Handbook distinguishes Intrusion Detection Systems (IDS) and Access Control Systems (ACS). IDS are a set of technologies and systems that define, observe, control, and sense entry into a defined controlled or secure area. ACS manage various combinations of entry, exit and/or movement through secure and controlled areas by the use of an identifiable token. In this Handbook, ACS are a subsystem that support IDS by enabling access by authorized personnel, preventing access by intruders, and interfacing with IDS to annunciate entry into controlled or secure areas. ACS cover the spectrum from simple keys to highly integrated biometrics controls. Since there are currently no ACS requirements or standards for transit facilities, examples and references are provided from other industries that can be applicable to transit systems. The Handbook contains a survey list used to quantify and qualify the ACS.

A broad range of audiences within the transit community can benefit from the Handbook to include general managers, senior executives, operational and technical managers, transit police, security personnel, and financial and procurement staff. The transit managers, in search of private industry assistance for their security system design, implementation, or upgrades, have the challenge of screening a very large number of companies. The Handbook also provides guidance on the type of questions and issues to be considered in the selection process for a capable, respected and reputable company that can provide the required security solutions.

The information in the Handbook was compiled based on a comprehensive literature search of commercial intrusion-detection system specifications and costs; a survey of major U.S. and international transit agencies; and on-site visits and interviews with general managers, senior staff, and security chiefs of selected major metropolitan transit facilities. The information received from surveys and interviews found that IDS and ACS presently used in transit systems are generally functioning as intended and are viewed as having satisfied their originally designed purposes. Several transit systems reported that intrusion detection applications also produced

secondary benefits in addition to their initial purpose. Cameras in facilities and vehicles have provided law enforcement agencies with evidence related to general criminal activity not necessarily related to the transit system. Transit employees have also become more aware of the role they can play to supplement and enhance intrusion detection and access control applications.

The Handbook provides comprehensive information on application and implementation of a wide range of IDS technologies to include, Fencing Systems, Barrier Systems, Lighting Systems, Video Systems, Access Control Systems, Sensor Systems, Identification Systems, Data Fusion, Display and Control Systems, Crisis Management Software, and a number of other systems.

For each of the technologies included in the Handbook, a user-friendly, brief discussion of the overall technology surrounding the device or application is provided, followed by a brief discussion of how it might be best applied as part of a security solution. Additional paragraphs provide information on system costs and other significant factors. Throughout the Handbook, where appropriate, tables have been included to provide a clear list of devices or applications for reference and comparison.

Tables with types of systems available, system description, system utilization, and system strengths and weaknesses are included. For the different intrusion detection and access control systems, references are provided with cost of implementation, cost of maintenance as a yearly percent of implementation, cost of training expressed as one time percent of implementation, and the estimated life expectancy of the system in years.

The heart of IDS is the various sensor systems used to detect violation into a protected area. Information for system design is used to choose and locate sensors. Information is provided on the types of available sensors, their application, and relative cost tables to include annunciation input, a description of IDS alarm annunciation and alarm classes, sensor processing, data fusion & display, and sensor types. Sensor characteristics are only part of the information required to choose an appropriate system. In addition, implementation, maintenance, training, and life expectancy must be included in the selection criteria. The Handbook provides a relative cost comparison of a sampling of various classes of sensors.

"Crisis Management Software" applies to an extremely wide (and continuously developing) variety of software applications from a widely diverse field of providing vendors or integrators that cover the complete gamut of crisis management. Most of these software applications fall into one of the six primary crisis management software categories that are described and discussed in the Handbook. Frequently, crisis management software packages will cover most potential crisis or hazard situations in a general way. Actual software titles, applications, and vendors number in the hundreds (if not thousands). In addition, hundreds of companies exist that will either custom tailor existing software to a requirement or create a custom software package for a specific or unique requirement. Therefore, it is recommended that research be conducted to identify the specific software application that best meets the crisis management requirements of a user.

Chapter 4 of the Handbook is designated to the steps in application and implementation of the intrusion detection and access control systems. The applications include general steps and data

on IDS technology systems. The Handbook discusses steps to create an effective and optimal intrusion detection system for public transit facilities. These sequential steps need to be followed before the effective application and implementation of IDS/ACS security technology. The steps include identifying a comprehensive list of assets, threats and vulnerabilities to the assets, risk and consequence assessment and determination of priorities. After the completion of the above steps, the process of applying IDS and ACS begins as a sequence of steps. The steps encompass design criteria, general design points, application steps, design steps, and design plans. Following the understanding of security technologies and completion of the above steps, a transit agency will be ready to implement improvements to their intrusion detection systems.

Strategies to enhance and upgrade intrusion detection invariably employ a combination of measures. There are no established standards that must be followed in every case. The actual order of implementation is often driven by a transit facility's local security architecture, overall security requirements, or direction from higher authority. Sometimes emphasis on a particular security technology area is in response to a specific incident or an identified weakness in that area.

The IDS technologies are developing and changing rapidly and the transit technical staffs have to keep abreast of the latest developments in these areas. Public transit professionals at all levels should continue to utilize the various networks of communication that are available and strive to establish continuous direct dialogue with other professionals who have current, applicable experiences.

CHAPTER 1. Introduction

Trespassing in transit agency properties such as tunnels, terminals, rail yards, and vehicles is an industrywide problem. Some intrusions have resulted in death or serious injury to the intruder and damage to agencies' infrastructure. Recent terrorist attacks have heightened security concerns, leading facility managers to deploy personnel to patrol or guard tunnels and other vulnerable areas. An effective intrusion detection system would reduce the need for security personnel at vulnerable areas, and thus, lower operating costs. Intrusion detection systems can deter and slow intruders and thereby reduce vandalism and damage to transportation property.

1.1 OBJECTIVE

The objective of this research is to develop a handbook for selecting and managing intrusion detection systems in the public transportation environment. The *Intrusion Detection for Public Transportation Facilities Handbook* ("Handbook") provides guidance on assessing system needs; developing system designs; and estimating system costs, benefits, and risks. The technologies and devices are applicable to the spectrum of public transportation facilities including transit facilities such as tunnels, bridges, buildings, power stations, transfer stations, rail yards, bus yards, and parking lots, as well as transit vehicles such as buses, trains, support vehicles, and special purpose vehicles. The applicable technologies are categorized in the Handbook to include performance specifications, implementation, and cost ranges.

1.2 AUDIENCE

This Handbook is directed toward a broad range of audiences within the transit community. The Handbook will enable general managers and other senior executives to quickly assess the technologies currently used in their agency versus the latest available options in intrusion detection. General managers and senior executives may also refer managers at operational levels to the Handbook to evaluate any necessary improvements. The Handbook will help these managers and technical staff in the transit community to quickly review the state of practice in intrusion detection technologies and focus on areas of interest to obtain information on technology, applications, costs, references, and other factors. The Handbook will also assist transit agency security personnel in developing new ideas for intrusion detection. Federal security and transit authorities can utilize this Handbook in assisting transit agencies in evaluating and upgrading intrusion detection technologies and in evaluating funding levels regarding the application of these technologies.

1.3 BASIC DEFINITIONS

Commonly available literature and technical source books have different and sometimes conflicting definitions of intrusion detection and related technologies. For the purpose of this Handbook the following definitions will apply.

Intrusion Detection System (IDS)
Intrusion detection systems are a set of technologies and systems that define, observe, control, and sense entry into a defined controlled or secure area. Defining systems contain and identify the secure area and include fences, barriers, and other civil structure such as buildings.

Observing systems provide methods for sensors and personnel to visually check a secure area and include lights and cameras. Controlling systems include access control, identification, and data fusion systems that control access and identify personnel.

Sensor systems are classically identified as IDS. These include an entire class of electronic systems (system) used to identify and alarm (detection) upon the entry (intrusion) of personnel into a secure area. Types and characteristics of sensors are described in Chapter 3.

Access Control System (ACS)
Access control systems are systems that manage various combinations of entry, exit and/or movement through secure and controlled areas by the use of an identifiable token. Managed entry means control of access to secure areas by operation of barriers and/or locking devices. Identifiable tokens could be a badge (Mag-strip, RF, etc.), biometric characteristic (fingerprint, iris scan, etc.), or a manually checked access list. Identification systems support IDS by providing a method to create and issue tokens, normally in the form of an access badge (card). For this Handbook, ACS is a subsystem that supports IDS by:

- Enabling access by authorized personnel
- Preventing access by intruders
- Interfacing with IDS to annunciate entry into controlled / secure areas

Additional Important Definitions
Important definitions and a source of confusion are the general types of IDS alarms.

There are two classes of alarms - Intrusion and Invalid.

Intrusion Alarm - annunciation of alarm resulting from detection of specified target attempting to enter into protected area

Invalid Alarms consist of three types:

Nuisance Alarm - annunciation of alarm by detection of stimuli that is not an attempt to enter into protected area

Environmental Alarm - annunciation of alarm resulting from environmental conditions

False Alarm - annunciation of alarm with no alarm stimuli

Additional information is found in Chapter 3 - Applicable Technologies and Appendix A - Glossary of Terms.

1.4 CONTENT OF THE HANDBOOK

The Handbook is designed for easy reference to the appropriate section as needed by the users. Although this Handbook is concise and brief, this section is provided as a guide to refer the users to the chapters that may be of most interest to them. Table 1 provides a brief description of the content of the Handbook.

Table 1 - Guide to the Content of the Handbook

Content	Discussion
Executive Summary	A three page executive summary of the scope and content of the Handbook
Chapter1: Introduction	Background information to this research that defines the audience, scope, and methodology in developing the Handbook. A checklist for General Managers and other users to determine the proper distribution and chapters of the Handbook for detailed review and implementation.
Chapter 2: Survey of Current Practices and Technologies	A summary of the current state of practice and technologies in major metropolitan transit agencies based on responses to a survey of several transit authorities.
Chapter 3: Applicable Technologies	A comprehensive list of intrusion detection technologies and information on applications, cost, and other factors as applied to transit operators.
Chapter 4: Steps in Applications and Implementation	General guidelines for application of intrusion detection systems and access control and other systems for transit agencies.
Chapter5: Management Policies and Procedures	A discussion on management trade-offs and policies and procedures with focus on implementation and solutions.
Chapter 6: Conclusion	A brief conclusion of the Handbook research.
Appendix	A glossary of terms, a valuable list of government and commercial references, a summary literature review, a copy of the survey of the transit agencies contributing to this research, and more detailed survey response information about the current state of practice and technologies in different aspects of a transit system.

Although most transit managers interested in intrusion detection technologies will benefit from reading the entire Handbook, the matrix in Table 2 provides a quick guide for selection of the most applicable chapters for different users.

Table 2 - Reference Matrix for Using the Handbook

Transit Staff / Chapter	General Managers & Senior Executives	Operations & Technical Staff	Transit Police & Security Personnel	Financial & Procurement Staff
Executive Summary	!	!	!	!
1. Introduction	!	!	!	!
2. Survey of Current Practices and Technologies		!	!	!
3. Applicable Technologies		!	!	
4. Steps in Applications and Implementation		!		
5. Management Policies and Procedures	!	!	!	!
6. Conclusion	!	!	!	!
Appendix		!	!	!

This Handbook discusses specifications, capabilities, and cost for a wide range of IDS technologies. The following tables provide a brief overview of the definitions and types of technologies that will be discussed in this Handbook.

Table 3 - Handbook Technology Definitions

IDS Technology	Definition
Fencing Systems	Contains and defines a secure or controlled area or perimeter
Barrier Systems	Contains, protects and defines a secure or controlled area or perimeter
Lighting Systems	Illuminates a secure area to increase sensor and personnel capabilities
Video Systems	Provide observation of a controlled or secure area or perimeter
ACS	Controls entry into a controlled or secure area or perimeter
Sensor Systems	Senses intrusion into an secure or controlled area
Identification Systems	Provide a method to identify authorized personnel
Data Fusion, Display and Control System (DFDCS)	Provide a method to fuse observation and sensor data
Crisis Management	System (usually software) to manage security incidents
Other Systems	Systems that support overall security that are not part of IDS

Table 4 - Handbook Technology Types

IDS Technology	Types	
Fencing Systems	Standard Chain Link ("cyclone") Fencing, Woven Wire Mesh Fencing, Welded-Wire Fencing, Rotating Sectional Top "Spikes", Barbed-Wire (top and/or side mounted), Razor-Wire (top and/or side mounted), Induced pulse (electrical) fencing, Ornamental Fence, Temporary Fences	
Barrier Systems	***Fixed Installation Barriers***	Steel or concrete framed or reinforced earthen barriers, Plastic (water- filled) or steel-reinforced concrete ("Jersey barrier"), Planter-styled security barriers, Steel "impaler-style" barriers, Concrete or metal bollards, Permanently installed concrete, cinder/concrete block, or brick wall-type barriers
	Deployable Barriers	Permanently installed "recessed-mounted" (in-ground) ramp-style vehicle barriers with chain reinforcements, Temporary or permanently installed "surface-mounted" ramp-style vehicle barriers with chain reinforcements, Hydraulically Deployable metal bollards, Traffic Controllers ("Tire Teeth")
Lighting Systems	Standard Incandescent, Tungsten Halogen, Reflector Lamps, Fluorescent, Compact Fluorescent, Solid State Light Emitting Diode (LED), Solid State Infrared (IR) LED, High Intensity Discharge (HID), Mercury Vapor, Metal Halide, High Pressure Sodium, Low Pressure Sodium, Sulfur	
Video Systems	***Imaging Devices***	Monochrome (Black & White), Tube, Solid State, Color, Convertible, Thermal Imaging System (TIS) Camera, Lens, Digital Video Recorder (DVR)
	Imaging Control	Zoom Lens, Optical, Digital, Pan and Tilt, Iris Control, Focus Control, Image Intensifiers, Security Mirrors, Wiper/Washer System, Heater/Cooler
Access Control Systems	Mechanical Key, Mechanical Combination, Electronic Combination - Key Pad, Electronic Credential, Barcode, Magnetic Stripe, Wiegand, Proximity, Smart Card, Proximity Smart Card, Other Cards, Biometric Credential, Finger Print – Optical, Finger Print – Capacitive, Finger Print – Ultrasonic, Iris Scan, Retinal Scan, Hand Geometry, Face Scan, Voice Print, Signature, Other Methods	
Sensor Systems	***Binary Sensor***	Balance Magnetic Switch, Breakwire, Call Box Alarm, Duress Alarm, Electric eye / Photo Electric Eye, Foil, Magnetic Switch, Mechanical Switch, Pressure Sensor / Mats / Switch, Security Screen
	Buried Sensors	Balanced Pressure Buried, Fiber Optic Cable, Geophone Buried, Ported Coax Buried Line
	Fence Sensor	Capacitive Cable, Electric Field / Electrostatic Field, Fiber Optic Cable / Mesh, Geophone / Microphone Fence, Taut Wire / Tension Sensor
	Fix Barrier / Wall Sensor	Capacitive Cable, Fiber Optic Cable / Mesh, Geophone Wall
	Infrared Sensors	Infrared Beambreak Detector, Passive Infrared Sensor / Detector (Heat sensor), Laser Scanning System
	Microwave Sensors	Microwave Bistatic, Microwave Monostatic, Radar, Radar Vehicle Detectors
Identification Systems	Photographic Badge System, Computerized User Data Base, Electronic Image Badge System (EIBS), Biometrics Badge System, Stand Alone Badge System, Networked Badge System, Integrated Badge System	
Data Fusion, Display and Control System	Coastal Surveillance and Display System (CSDS), Security Data Management System (SDMS), OmniDirectional Intelligent Tracking Software, Visual Security Operations Center (VSOC)	
Crisis Management Software	Emergency Management, Business Continuity, Disaster Recovery, System Backup or Restoration, Environmental, Health, and Safety (EH&S), Vulnerability Assessment (VA)	
Other Systems	Asset Tracking Systems, Computer Security, Contingency Planning, Data Backup Policy Methods Procedures, Data Transmission Systems, Disaster Recovery Planning, Document Protection & Destruction, Drug / Substance Abuse, Facility "Hardening", Fire & Life Safety, Personnel or Background Checks, Power and Power Supplies, Power Back Up Systems, Toxic Sensors, Training (Periodic, Special and Emergency), Vehicle Inspection	

1.5 SCOPE

The information in the Handbook applies to the following transit facilities and vehicles:

1. *Transit Facilities*
   - Tunnels
   - Bridges
   - Buildings (control centers, maintenance facilities, parking structures, storage facilities)
   - Power stations
   - Terminal/transfer facilities above and below ground
   - Rail/bus yards
   - Parking lots

2. *Transit Vehicles*
   - Trains/rail cars
   - Buses
   - Service/support vehicles
   - Special purpose vehicles
   - Paratransit vehicles

1.6 METHODOLOGY

The research to compile this Handbook involved the following general methodology:

1. Conducted a literature search of the information available on intrusion detection systems. The search included literature on the technologies implemented in major metropolitan transit authorities as well as commercial detection technologies as applied by the government and the private industries.
2. Conducted a survey of major transit agencies to assess the state of practice and technologies currently utilized, pros and cons of such systems, and capital and operating cost information. A similar survey was conducted with several international transit agencies.
3. Conducted on-site visits with selected major metropolitan transit facilities. Interviewed general managers, senior staff, and security chiefs of each agency to gain insight on management issues, realities of implementation and competing costs of applying security upgrades, and operational issues of transit agencies.
4. Developed categories of applicable intrusion detection devices and compiled detailed information of the technology, applications, and cost.
5. Collected specifications and cost information on each group of applicable technologies, including training and calibration requirements for effective operation.
6. Highlighted trade-offs and decision points facing the senior managers at the policy level and how they play out in the procurement venue.
7. Focused on developing a concise and user-friendly Handbook with a broad range of audiences within the transit environment.

1.7 ASSUMPTIONS

It is assumed that transit systems have already implemented some degree of security in their facilities and will use this Handbook to compare their intrusion detection systems to current state of the art technologies or to consider selected upgrades. It is also assumed that the users of the Handbook have some degree of security experience in the use of intrusion detection and access control systems. This Handbook provides information on the application of intrusion detection systems and introduces the users to many other related resources. The application and cost factors vary greatly based on facility size, geographic area, site-specific conditions, product availability, and many other factors. In the decision-making process of applying any of these systems, transit systems need to obtain details of the available systems, assess their degree of effectiveness, and obtain more specific application and implementation information from selected designers and vendors.

1.8 CAUTIONARY NOTE

There are hundreds (if not thousands) of companies, both small and large, in the United States and abroad that design security equipment and develop software or provide security services and support. Many are reputable businesses with a good standing in the security industry and excellent past performance records - but some are not. Since September 11, 2001, and following subsequent announcements regarding Homeland Defense spending projections, there has been a proliferation of companies proclaiming to be "security experts."

In searching for private industry assistance in any transit security system design, implementation, or upgrade, security managers should endeavor to keep in mind some of the following considerations for the candidate companies:

- Line of products or support. What does the company provide?
- History in the industry. How long have they been in business?
- Breadth of expertise. What variety of security-related services do they provide or perform?
- Record of past performance. What customers has the company previously supported and are those customers satisfied?
- Does the company provide a single solution? What else is required to ensure successful operation of the technology?
- What is the ability of company to integrate products in an overall effective solution?

By asking these and other questions and by researching the security marketplace, the transit facility security managers can be assured of finding a capable, respected and reputable company that can provide the needed security assistance or product to meet their needs.

CHAPTER 2. Survey of Current State of Practice and Technologies in Transit Systems

2.1 SURVEY OF TRANSIT SYSTEMS

Transit systems in the United States and selected international areas were surveyed to determine the following:

Current applications of intrusion detection
- Experiences related to satisfaction, reliability, costs, and operational impacts
- Need for technology development to meet future needs

The survey questionnaire was intended to gather information related to intrusion detection applications for any and all public transportation facilities as well as vehicles.

Public transportation facilities included the following:
- Administrative Buildings
- Maintenance Facilities (Bus & Rail)
- Storage Facilities
- Rail Yards
- Operational Control Centers
- Power Stations
- Train Control Areas
- Stations
- Tunnels
- Bridges
- Terminals/Transfer Facilities
- Operating Right-of-Way
- Parking Lots/Structures

Public Transportation Vehicles included the following:
- Trains/Rail Cars
- Buses
- Service/Support Vehicles
- Special Purpose Vehicles
- Paratransit Vehicles

Intrusion Detection Applications included:
- Video Surveillance
- Access Control Systems
- Sensors
- Alarm Systems
- Fences
- Barriers
- Lighting
- Human Resources
- Other

The survey questionnaire consisted of twenty-one questions and associated tables for responses. Additional information on specific items related to several questions was also solicited.

Response to the survey was over 90% and produced an extensive amount of data. Follow-up telephone discussions with several transit systems provided additional information and clarity to the basic survey responses. Finally, selected site visits were conducted to provide an in-depth understanding of the state of the practice and physical inspections of intrusion detection applications.

The next section is a general introduction and synthesis on the current state of the practice, derived from the collective information received from all sources. Specific templates describing applications and experiences with intrusion detection applications for various public transportation facilities and vehicles are contained in Appendix E of this Handbook.

2.2 CURRENT STATE OF PRACTICE

2.2.1 Introduction

Public transit systems are intended to move large numbers of people quickly and efficiently, and therefore, are designed to offer a high degree of user access. While transit vehicles and facilities such as stations, terminals, and parking lots must be fully accessible to customers, many other transit facilities such as bridges, tunnels, rights-of-way, maintenance and storage facilities, power stations, train control, and operational control centers must be designed to restrict access to authorized personnel only. Administrative facilities must allow some level of public access with high degrees of control. Intrusion into public transportation facilities poses significant safety and liability risks, potential theft and vandalism, service disruptions, and opportunities for terrorist activities.

2.2.2 State of the Practice - General

Intrusion Detection Applications

Devices such as sensors, detectors, alarms, and surveillance cameras are collectively called Intrusion Detection Systems or simply IDS. IDS are installed by transit systems to annunciate intrusion in various facilities and vehicles. Access Control Systems, or ACS, are used by transit systems to control and limit access to only authorized and qualified personnel. IDS and ACS work together to promote the improvement of safety, provide for enhanced security, reduce hazards, curb vandalism and crime, and raise customer perceptions about system security and service quality. This layered approach allows the individual device or application to reinforce others.

Many types of IDS are currently in use and include both high- and low-technology solutions. Systems from simple magnetic door switches to sophisticated Infra-Red (IR) motion sensors are used to indicate intrusion of personnel into protected or monitored areas. IDS also include low-technology applications such as fences, barriers, and lighting used to identify and contain protected areas. While these applications cannot by themselves detect intrusion, they can provide indication of intrusion or ill intent. For example, a fence with a hole cut in it would most likely indicate that someone has gained unauthorized access to the zone protected by the fence. ACS utilizes methods and technologies from personnel checks to high-technology biometric readers to identify and authorize entry of personnel into protected areas. IDS and ACS along with communications systems, training, methods, human

resources, procedures, analysis and more provide a complete package to detect and prevent unwanted intrusions in transit facilities. Details of the types of systems available are contained in Chapter 3 of this Handbook.

Applications of IDS and ACS work collectively to enhance both safety and security. ACS attempt to prevent intrusion into secure areas, while IDS alert operational and security personnel when an intrusion actually occurs. Actual intrusions, as well as nuisance and other alarms, are expensive for transit systems, which experience service delays and the expense of dispatching personnel to the site of an intrusion. Proper application of IDS and ACS technologies can contribute to an improved financial condition of a transit agency by preventing accidents, minimizing service disruptions, and avoiding damage created by intruders.

IDS and ACS are generally installed as preventive systems, but in several cases they are implemented in response to specific events or incidents. Additional design steps for installing specific systems are outlined in Chapter 4 of this Handbook. In summary, the standard steps are to identify the asset to be protected, identify the threat, identify the vulnerabilities, assess the risk and determine priorities, and then apply IDS and ACS. Ultimately a goal of the IDS and ACS is to avoid delays to the system by preventing the entry of unauthorized personnel into protected areas. Service delays have associated service quality and financial ramifications that can be presented as a business case to help justify investment into IDS and ACS technologies.

Transit System Experiences

The information received from surveys, telephone interviews, and site visits found that IDS and ACS presently used in transit systems are generally functioning as intended and are viewed as having satisfied their originally designed purposes. Exceptions to this general level of satisfaction exist with some digital video surveillance systems and false and nuisance alarms from sensing devices. Technology advancements in these areas are improving system reliability and assist in preventing false and nuisance alarms. Regardless of the problems experienced, most systems indicate that they would select the same application or product with technology upgrades that incorporate increased and improved functionality.

Several transit systems reported that intrusion detection applications also produced secondary benefits in addition to their initial purpose. Cameras in facilities and vehicles have provided law enforcement agencies with evidence related to general criminal activity not necessarily related to the transit system. Transit employees have also become more aware of the role they can play to supplement and enhance intrusion detection and access control applications.

Intrusion detection applications have generally not had adverse effects on transit operations. There have been occasional nuisance alarms that can result in both service disruptions and the commitment of employee time to respond to the problem. In many instances, the nuisance alarms resulted from employees accidentally triggering an alarm (showing the need for additional training).

Transit systems are using both customized and commercial off-the-shelf (COTS) products in their intrusion detection applications. These COTS products typically allow for modest modifications and custom configuration (computer display maps, etc.) to fulfill the transit system's standards and requirements. These configurable COTS products are less expensive than the purely customized applications that are rarely used in transit applications.

Life expectancy of intrusion detection applications depends on the type and complexity of the system and the environmental installation conditions. Fences, barriers, and lighting have a life expectancy of 20+ years. Access control systems and simple alarm systems can expect to last for 10 to 15 years. Advanced sensors and video systems typically have a life expectancy of 5 to 7 years. Transit agencies must plan for upgrades and replacement of all systems, particularly those high-technology systems with shorter life expectancy. Upgrades may include replacement of older equipment, VHS tape conversion to digital video recorders (DVR), and anti-climb features/motorized gate technology applied to yard gates and fences. These upgrades must be balanced with other system needs and the available funding to make needed improvements.

Following the review of security protocol after September 11, 2001, transit systems made several modifications to their IDS and ACS. Additional fencing, gates, lighting, barriers, video surveillance and a greater use of human resources have all occurred. Specialized applications related to high vulnerability areas such as compressed natural gas (CNG) storage facilities, bio-chemical detection (not in the scope of this Handbook) and access control to administrative buildings were implemented. Many transit systems have developed formal plans and procedures to continually assess vulnerability and conduct quality performance audits on facilities and operations.

Other modifications have also been made through the years since the applications were originally installed. Some were made in response to specific events or incidents, while most were intended to prevent problems in the future. Many modifications were triggered by the development of new or improved technology devices or systems that were far superior to older products.

Due to the limited cost data received from the survey of transit systems, information on costs was instead collected from vendor and manufacturer sources. That information is provided Chapter 3 of this Handbook.

Future Needs

The largest long-term impact of increased security is the additional labor required to repair, service, and monitor intrusion detection systems. The cost impact of these three areas is beginning to be addressed by the application and implementation of technological advances. These advances are leveraged to decrease life cycle costs by increasing system reliability and also lowering routine service requirements.

Continued advancement in technology has already greatly decreased life cycle costs. Examples include the following: replacement of tube camera systems with solid state imagers, upgrade to electronic from electro-mechanical systems, and even simple items such as replacing mechanical switch contacts for sealed magnetic devices. The trend of advancement will continue to provide longer system life and thus lower costs. This trend however requires, in the event of subsystem failure, the replacement of large subsystems instead of smaller scale component replacement. Transportation facilities therefore must plan in budgetary and maintenance cycles for this large-scale subsystem change out.

More difficult is the minimizing of labor required to monitor intrusion detection systems. As transportation organizations know, it is very labor intensive to observe and interpret video signals and system alarms. The first step of lowering labor costs is to add video monitoring for remote

observation of intrusion alarms. This allows operators and security personnel to check alarms without the dispatch of security personnel. The next step is to allow video systems to monitor for intrusion without the assignment of labor to continuously observe video pictures.

A method to automate the process is currently starting to be addressed. By leveraging research and development funded by military sources, technology and software systems can now be utilized to perform both repetitive and complex video monitoring tasks. These technologies employ advanced methods of video motion detection that eliminate most of the invalid alarms experienced with current systems.

Transit systems follow technology development trends in all areas of safety and security. They are cautious of higher costs and poor reliability often associated with first-generation technology products and will usually wait for lower cost, improved versions to be developed. Transit systems are labor intensive by their very nature and are concerned with IDS and ACS that also require a high level of maintenance and human resource intervention. The increased concern for security on transit systems will result in an increase in the level of investment made in IDS and ACS applications. New technologies will have an increased presence in these applications.

CHAPTER 3. Applicable Technologies

Technology Summaries/Specifications/Capabilities/Costs

This chapter outlines the various Intrusion Detection and Access Control System hardware and software devices or applications that a transit system might consider as part of a security program. For each of the following sections, where applicable, a brief discussion of the overall technology surrounding the device or application is provided, followed by a brief discussion of how it might be best applied as part of a security solution. Additional paragraphs provide discussions of system costs and other significant factors. Throughout this chapter, where appropriate, tables have been included to provide a clear list of devices or applications for review and comparison.

3.1 FENCING SYSTEMS

Fencing systems are utilized for the following functions:

1. Boundary definition
2. Aid in control of screening and entry for access control
3. Support security detection and assessment
4. Deter casual intruders
5. Causes an intruder to perform an overt act that demonstrates intent
6. Briefly delays intruder

3.1.1 Technology

There are many types of fencing systems. Some are designed primarily for temporary installation for short-term events and others are designed for longer-term, permanent installation. Frequently, a combination of the two types will best suit a particular facility's security needs. Key factors in fence selection are material construction (plastic, aluminum, steel); fence design (woven or welded-mesh, straight or ornamental-shaped metal bars); fence height (usually 3 to 12-feet, sometimes higher); and installation method (posts driven into ground, poured into concrete, or welded panels). While these factors are the most common, there are almost as many installation methods as there are types of fencing systems. Obviously the key to an effective fencing system is choosing the right type of fence to meet the system requirements.

Tables 5 and 6 provide a reference to available technologies and systems. Columns are as follows:

- Fencing System – A list of the types of fencing systems available
- System Description – A short description of the fencing system
- System Utilization – The application of the fencing system
- Systems Strengths – Positive attributes of the fencing system
- System Weaknesses – Negative attributes of the fencing system

Table 5 - Fencing Systems

Fencing Systems	System Description	System Utilization
Standard Chain Link ("cyclone") Fencing	Standard galvanized steel Chain Link fencing as used in numerous instances to provide a low to medium level of security at reasonable cost	To provide temporary or permanent perimeter definition around large or small facilities, buildings or exclusion zones
Woven Wire Mesh Fencing	Woven wire-mesh is similar to chain-link but has varying sizes of mesh and different colors and coatings	To provide temporary or permanent perimeter definition around large or small facilities, buildings or exclusion zones
Welded-Wire Fencing	Welded-wire is welded at every joint or wire-crossing. The varied-size mesh is usually rectangular or square in shape. Mesh openings can be made too small to offer a toehold or handgrip	To provide temporary or permanent perimeter definition around large or small facilities, buildings or exclusion zones
Rotating Sectional Top "Spikes"	Rotating sections (usually 3 to 4-feet in length) of sharp, "spiked" devices mounted horizontally along the top of fence segments	Presents a serious puncture hazard to anyone attempting to climb over the top of a fence segment
Barbed-Wire (top and/or side mounted)	Standard style of barbed wire that is placed in single-strand, multi-strand, or coil along the top and/or side of a vertical barrier (wall or fence). Coils can also be stretched or stacked along the ground	Used to complement existing barriers, and to preclude scaling through use of sharp barbs. Used on the ground, provides a effective barrier to all but experienced professionals
Razor-Wire (top and/or side mounted)	Coil style of barbed wire produced by cutting and bending flat sheets of metal. Stored as round compressed stacks. Placed in single-coil or multi-coil on the top and/or side of a vertical barrier (wall or fence). Coils can also be stretched or stacked along the ground	Used to complement existing barriers, and to preclude scaling through use of sharp razor-shaped edges. Used on the ground, provides a effective barrier to all but experienced professionals
Induced pulse (electrical) fencing	Multi-wire electrical fencing providing a high-voltage but short-duration (~1-sec) electrical "pulse"	Best used to meet "high-security" requirements in authorized localities. Provides a sharp but safe electrical jolt.
Ornamental Fence	Hot-dipped galvanized steel, wrought iron or aluminum "bars"	Designed to provide low to medium security while maintaining aesthetic value
Temporary Fences	Chain-link fencing, coiled or stretched barbed wire, coiled or stretched razor wire, "hedge hog" obstructers, etc.	Deployed for short or longer-term "temporary use" to restrict vehicle or foot traffic

Table 6 - Fencing System Strengths and Weaknesses

Fencing Systems	System Strengths	System Weaknesses
Standard Chain Link ("cyclone") Fencing	Low to medium cost, normally requires little to no maintenance, easily configured to meet almost any size or shape requirements	Easily cut with bolt cutters or strong shears, can be easily scaled, and must be "framed" top, bottom and vertically at points along its length to provide adequate security
Woven Wire Mesh Fencing	Medium cost, normally requires little to no maintenance, easily configured to meet almost any size or shape requirements	Easily cut with bolt cutters or strong shears, can be scaled, and must be "framed" top, bottom and along its length to provide adequate security
Welded-Wire Fencing	Medium to higher cost, normally requires little to no maintenance, easily configured to meet almost any size or shape requirements	While easily cut with bolt cutters or strong shears, requires many cuts to actually create an opening. Smaller mesh makes scaling difficult. Must be "framed" top, bottom and along its length to provide adequate security
Rotating Sectional Top "Spikes"	Provides a strong physical and psychological barrier to all but experienced professionals.	Not permitted in some jurisdictions and may open user to potential liability and/or litigation
Barbed-Wire (top and/or side mounted)	Provides a strong physical and psychological barrier to all but experienced professionals. Easily deployed in long coils for temporary security use	Can be easily cut with proper tools and solitude. Protective clothing is required for deployment, attachment, or anchoring to barriers or the ground
Razor-Wire (top and/or side mounted)	Provides a strong physical and psychological barrier to all but experienced professionals. Easily deployed in long coils for temporary security use. Higher security than standard barbed wire.	Can be cut with proper tools and solitude. Protective clothing is required for deployment, attachment, or anchoring to barriers or the ground
Induced pulse (electrical) fencing	Provides effective physical and psychological barrier for potential intruders, and can be combined with additional sensors	Not permitted in some jurisdictions and may open user to potential liability and/or litigation
Ornamental Fence	Unobtrusive, looks good, avoids too much of a "security" appearance	May provide minimal level of security if appearance over function is stressed
Temporary Fences	Low cost, rapidly deployed, easily configured for wide variety of requirements	Offers limited protection, and may require protective clothing to deploy

3.1.2 Applications

Temporary fences are usually less secure, while permanent fences will frequently include tamper-proof hardware as part of their installation. Larger mesh sizes make it easier to cut or to get a toe- or finger-hold (making them easier to climb), while smaller mesh sizes are harder to climb and more time-consuming to cut. The heavier the gauge of metal wire used in the mesh, the harder it is to cut and the longer it will last. Some combination fence systems are actually part-wall and part-fence, with the lower part of the system made of steel or concrete, with the top portion actually being "fence". This type of fencing system has the added benefit of providing some degree of "barrier" protection if properly anchored to the ground.

3.1.3 Costs

Fencing System characteristics are only part of the information needed for the choice of an appropriate system. In addition, implementation, maintenance, training, and life expectancy must be included in the selection criteria.

The following table provides a summary of costs. Please note that even though materials costs are similar throughout the US, labor costs vary as much as 3 times and this will affect the amounts shown in the tables. Each authority will need to include this factor in implementation and support of the deployed systems.

Table 7 provides a reference to rough systems costs.

- Fencing System – List of Fencing System types
- Cost of Implementation – Cost of installing system
- Cost of Maintenance – Operational costs expressed as a yearly % of implementation
- Cost of Training – Expressed as one time % of implementation
- Life Expectancy – Estimated system life expectancy in years

Table 7 - Fencing Systems Technologies Cost Matrix

System	Rough Cost of Implementation	Comments	Cost of Maintenance & Operation % per year	Comments	Cost of Training % one time	Comments	Life Expectancy
Standard Chain Link ("cyclone") Fencing	$20 to $25 per linear foot installed	Varies greatly with region and amount required	Normally less than 5%	Minimal maintenance required	0%	No training required	25+ years
Woven Wire Mesh Fencing	$25 to $45 per linear foot installed	Varies greatly with region and amount required	Normally less than 5%	Minimal maintenance required	0%	No training required	25+ years
Welded-Wire Fencing	$25 to $45 per linear foot installed	Varies greatly with region and amount required	Normally less than 5%	Minimal maintenance required	0%	No training required	25+ years
Rotating Sectional Top "Spikes"	$8 to $12 per 4-5-foot section installed	Varies greatly with region and amount required	Normally less than 5%	Basic maintenance and upkeep required	Less than 5%	Minimal training required	10+ years
Barbed-Wire (top and/or side mounted)	$2 to $3 per linear foot installed	Varies with type, style, and amount required	Normally less than 5%	Minimal maintenance required	Less than 5%	Minimal training required	10+ years
Razor-Wire (top and/or side mounted)	$3.50 to $ 5 per linear foot installed	Varies with type, style, and amount required	Normally less than 5%	Minimal maintenance required	Less than 5%	Minimal training required	10+ years
Induced pulse (electrical) fencing (not always permitted by law in some localities)	$45-plus per linear foot installed	Varies greatly with region and amount required	5%	Basic maintenance and upkeep required	Less than 5%	Minimal training required	15+ years
Ornamental Fence	$50-plus per linear foot installed	Varies greatly with region and amount required	5 to 10%	Basic maintenance and upkeep required	0%	No training required	20+ years
Temporary Fences	$5-10per linear foot installed, per 3 to 6-month rental	Varies greatly with region and amount required	5 to 15%	Basic maintenance and upkeep required	Less than 5%	Minimal training required	10+ years

3.1.4 Other Factors

There are other factors that must also be considered in the implementation of a fencing system. These include, but are not limited to the following:

- Requirement for fencing system type - should it be basic chain-link ("cyclone") fencing or is a higher-security welded-wire mesh type of fence required? Is the fence to merely guide pedestrian traffic or is it to inhibit (or preclude) entry into designated areas? Does the fence need to preclude visibility through the fence?
- Installation plans - is the installation temporary or permanent, and who will do the installation, and when? How much fencing will be required and what areas or zones will require fencing? Are any special styles, materials or colors required? Plastic strips are available in many colors to weave into the mesh. Some wire-mesh fence systems are available with a colored plastic coating. Should the fencing have top-mounted barbed or razor wire, or a special device (e.g. spikes)? Do surveillance cameras have a clear view of the fence?
- Local ordinances - codes may require or preclude certain types of fencing systems - for example, unprotected electrified fences are not permitted in many localities

3.2 BARRIER SYSTEMS

3.2.1 Technology

There are many types of barrier systems. Some barriers are used to guide pedestrian traffic flow, or are specifically designed to block smaller objects of certain sizes, such as the safety barriers (bollards) that stop large luggage from being taken or pulled onto powered walkways or escalators. For the purpose of this document, the barriers being addressed are primarily designed to preclude physical entry into a designated security zone by vehicles. Most barriers used in this type of security applications are designed to withstand the damaging forces caused by hitting or ramming the barrier with a vehicle. In some cases, these barriers will withstand the extreme force of a large loaded truck moving at speed of over 50 mph. The key to an effective barrier system is choosing the right type of barrier to meet the facility's specific security requirements.

Tables 8 and 9 provide a reference to available technologies and systems. Columns are as follows:

- Barrier System – A list of the types of barrier systems available
- System Description – A short description of the barrier system
- System Utilization – The application of the barrier system
- Systems Strengths – Positive attributes of the barrier system
- System Weaknesses – Negative attributes of the barrier system

Table 8 - Barrier Systems

Barrier Systems	System Description	System Utilization
Fixed Installation Barriers		
Steel or concrete framed or reinforced earthen barriers	Simple steel and concrete framework backfilled with soil, and topped with sod	Best used in open areas with plenty of space and when cost is an issue. Can be used to "route" or "direct" vehicle or pedestrian traffic
Plastic (water- filled) or steel-reinforced concrete ("Jersey barrier")	Simple molded plastic (filled with water) or steel-reinforced concrete barrier available in various styles, lengths, shapes and colors	Placed as protective barriers where needed. Can be arranged end-to-end, side-by-side, or even stacked for increased security. Can be used to "route" or "direct" vehicle or pedestrian traffic
Planter-styled security barriers	Steel reinforced concrete "shell" that is backfilled with soil for added protective weight	Prevents vehicle intrusion. Protects walkways, fences, guard booths, important equipment and prevents driving around other barriers. Can be used to "route" or "direct" vehicle or pedestrian traffic
Steel "impaler-style" barriers	Designed to roll backward upon impact, impaling the vehicle on the underside, subsequently acting as an extreme friction anchor. 42-inches high and available in 10- or 12-foot lengths	Placed wherever needed, installed slightly below grade, and backfilled in-place with concrete. Barriers can be interconnected for extended lengths
Concrete or metal bollards	Vertically installed metal (preferably steel) "crash tube" with the lower base extending into the ground, and constructed of solid steel, or hollow tube filled with reinforced concrete. In use in numerous military and commercial applications	Inhibits vehicle intrusion. Protects walkways, fences, guard booths, important equipment and prevents driving around other barriers. Bollards come in several security levels and are usually installed in linear arrays. Can be used to "route" or "direct" vehicle or pedestrian traffic. Frequently adorned with warning lights
Permanently installed concrete, cinder/concrete block, or brick wall-type barriers	A vertically constructed and installed reinforced concrete, cinder/concrete block, or brick wall of a specified height, thickness and material to meet a specified level of security	Installed around a security zone or high-value asset requiring protection
Deployable Barriers		
Permanently installed "recessed-mounted" (in-ground) ramp-style vehicle barriers with chain reinforcements	A rugged 5- to 24-foot wide steel ramp raised at an approximate 27-degree angle, with a forward edge-height of approximately 3 feet. The leading, raised edge of the ramp impacts an intruding vehicle, completely stopping and/or destroying the vehicle. These ramp systems weigh between 2,500 to 12,000-pounds and are installed flush-mounted in the surface of the road	Upon impact, completely stops and/or disables the unauthorized vehicle. The ramp barrier system is raised or lowered either manually or automatically (based on access being granted) through use of computer-controlled electrical or hydraulic systems.
Temporary or permanently installed "surface-mounted" ramp-style vehicle barriers with chain reinforcements	A rugged 5- to 24-foot wide steel ramp raised at an approximate 27-degree angle, with a forward edge-height of approximately 3 feet. The leading, raised edge of the ramp impacts an intruding vehicle, completely stopping and/or destroying the vehicle. These ramp systems weigh between 2,500 to 12,000-pounds and are installed on the top surface of the road	Upon impact, completely stops and/or disables the unauthorized vehicle. The ramp barrier system is raised or lowered either manually or automatically (based on access being granted) through use of computer-controlled electrical or hydraulic systems.
Hydraulically Deployable metal bollards	Subsurface vertically installed metal "crash tube". In unsecured position devices are flush with surface, once deployed part of tube is above surface with the lower part extending into the ground. Constructed of solid tubular steel, can be filled for added strength. In use in numerous military and commercial applications	Inhibits vehicle intrusion. Protects walkways, fences, guard booths, important equipment and prevents driving around other barriers. Bollards come in several security levels and are usually installed in linear arrays. Can be used to "route" or "direct" vehicle or pedestrian traffic.
Traffic Controllers ("Tire Teeth")	Approximate 1 inch wide by 4 inch long teeth are used to cut / shred vehicle tire. Metal teeth that are either spring mounted to allow safe one way travel or retractable to allow two way travel.	Prevention of wrong way traffic flow (parking applications) and deployable to flatten tires if vehicles cross security access point.

Table 9 - Barrier Systems Strengths and Weaknesses

Barrier Systems	System Strengths	System Weaknesses
Fixed Installation Barriers		
Steel or concrete framed or reinforced earthen barriers	Maximum protection at lowest cost, if the required space is available	Requires some lawn maintenance if earthen section is planted with sod or hedges
Plastic (water- filled) or steel-reinforced concrete ("Jersey barrier")	Highly configurable and effective protection at low to moderate cost and very low maintenance. Empty water-filled units weigh less than 200-pounds, are easy to transport, and come in a variety of colors	Plastic water-filled versions do require water source and drainage area, water freezing problems in cold weather. Concrete versions are heavy and require substantial forklift or crane for proper placement. For maximum protection barriers need to be physically attached to mounting surface.
Planter-styled security barriers	Aesthetically tailored with unlimited number of sizes, styles, and finishes.	Large, heavy, and difficult to relocate once filled with soil. Soil removal is time consuming
Steel "impaler-style" barriers	Easily installed, not very heavy or hard to move until back-filled with concrete. Multiple units can be connected for extended barrier lengths	May need to be replaced, or reinstalled, after actual use. Still allows target vehicle to travel short distance into security zone. May cause vehicle fire or injury to occupant
Concrete or metal bollards	Very effective solution. Can stop and/or destroy 15,000-pound (GVW) vehicles moving up at speeds up to 50 MPH. Inexpensive to install and maintain using local materials and experience. Aesthetically tailored with unlimited number of sizes, styles and finishes.	Outer aesthetic covering can become damaged and need to be replaced. Facility may require engineering analysis to ensure robust design for specific needs.
Permanently installed concrete, cinder/concrete block, or brick wall-type barriers	Easily installed by any construction firm and provides a clear line of demarcation. Actual wall construction material, thickness and height can be selected to meet any facility requirement or security level	Permanent installation - cannot be easily relocated. Possible high cost is dependent on security level. Facility may require engineering analysis to ensure robust design for specific needs.
Deployable Barriers		
Permanently installed "recessed-mounted" (in-ground) ramp-style vehicle barriers with chain reinforcements	Assigned various government certifications (e.g. K12, L2) to stop and/or destroy vehicles ranging up to 20,000 pounds (GVW) moving at speeds up to 70 MPH. When in the lowered position, the barrier is flush with the roadway. One of the most effective barriers on the market. Rises in 2-seconds and is usually operational even after actual vehicle impact	Requires modification to ground surface for installation. May need to be replaced, or merely reinstalled, after actual use - dependent on speed and weight of vehicle stopped or destroyed. Still allows target vehicle to travel short distance into security zone. May cause injury to occupant or vehicle fire
Temporary or permanently installed "surface-mounted" ramp-style vehicle barriers with chain reinforcements	Assigned various government certifications (e.g. K12, L2) to stop and/or destroy vehicles ranging up to 20,000 pounds (GVW) moving at speeds up to 70 MPH. When in the lowered position, the barrier is nearly flush with the roadway. One of the most effective barriers on the market. Rises in seconds and is usually operational even after actual vehicle impact	May need to be replaced, or merely reinstalled, after actual use - dependent on speed and weight of vehicle stopped or destroyed. Still allows target vehicle to travel short distance into security zone. May cause vehicle fire or injury to occupant
Hydraulically deployable metal bollards	Very effective solution. Controlled by security system for security reconfiguration as desired. Aesthetically tailored with many styles and finishes.	Deployable / retractable model more complex and expensive. Damage problems from accidental deployment.
Traffic Controllers ("Tire Teeth")	Common systems in parking lot applications. Easily installed by construction companies. Numerous vendors and supplies.	Inadvertent tire damage from vehicles backing up or traveling in the wrong direction.

3.2.2 Applications

While the numerous types of Barrier Systems allow them to be applied in many ways, they are primarily used in a security role to block entrance to an area by vehicles. They can be placed at a facility's gates or entrances (vehicle "checkpoints") to stop intruding vehicles; around security guard booths; between designated parking areas and buildings; around high-value facilities or assets; or placed as a protective barrier around temporary events. Barriers can be manned (such as those in use at pedestrian or vehicle gates) or unmanned, such as traffic controllers ("tire teeth"). The applications are as varied as the systems and can be combined to provide an even more effective Barrier System.

3.2.3 Costs

Barrier System characteristics are only part of the information required to choose an appropriate system. In addition implementation, maintenance, training, and life expectancy must be included in the selection criteria.

The following table provides a summary of costs. Please note that even though materials costs are similar throughout the US, labor costs vary as much as 3 times and this will affect the amounts shown in the table. Each authority will need to include this factor in implementation and support of the deployed systems.

Table 10 provides a reference to rough systems costs.

- Barrier System – List of Barrier System types
- Cost of Implementation – Cost of installing system
- Cost of Maintenance – Operational costs expressed as a yearly % of implementation
- Cost of Training – Expressed as one time % of implementation
- Life Expectancy – Estimated system life expectancy in years

Table 10 - Barrier Systems Cost Matrix

System	Rough Cost of Implementation	Comments	Cost of Maintenance & Operation % per year	Comments	Cost of Training % one time	Comments	Life Expectancy
Fixed Barriers							
Steel or concrete-framed or reinforced earthen barriers	$40 a cubic yard and up	Requires construction contractor	Less than 5%	Low cost to maintain	0%	No training required	30+ years
Plastic (water-filled) or steel-reinforced concrete ("Jersey barrier")	$100 to $500 each	Requires equipment for placement	Less than 5%	Low cost to maintain	0%	No training required	20+ years
Planter-styled security barriers	$500 to $1K	Requires equipment for placement	Less than 5%	Low cost to maintain	0%	No training required	20+ years
Steel "impaler-style" barriers	$100 to $150 a linear foot	Requires equipment for placement	Less than 5%	Low cost to maintain	0%	No training required	15+ years
Concrete or metal bollards	$100 to $500 each	Requires construction contractor	Less than 5%	Low cost to maintain	0%	No training required	15+ years
Permanently installed concrete, cinder/concrete block, or brick wall-type barriers	$4 a square foot and up	Requires construction contractor	Less than 5%	Regular "wall" - low cost to maintain	0%	No training required	30+ years
Deployable Barriers							
Permanently installed "recessed-mounted" (in-ground) ramp-style vehicle barriers with chain reinforcements	$25k to $50K each	Permanently installed	5 to 10%	Requires some work - mostly cleaning & lubrication	10%	Minimal training required to operate	15+ years
Temporary or permanently installed "surface-mounted" ramp-style vehicle barriers with chain reinforcements	$10K to $25K each	Temporary or permanently installed	5 to 10%	Requires some work - mostly cleaning & lubrication	10%	Minimal training required to operate	15+ years
Hydraulically deployable metal bollards	$15K to $40K for set of 4 or more	Permanently installed	5 to 10%	Requires some work - mostly cleaning & lubrication	5%	Minimal training required to operate	20+ years
Traffic Controllers ("Tire Teeth") either permanently installed or "pull-out" for emergency use to stop vehicle	$2K to $15K each	Permanently installed or quickly deployed	Less than 5%	Low cost to maintain	5%	Minimal training required to operate	10+ years

3.2.4 Other Factors

There are other factors that must also be considered in the implementation of a barrier system. These include, but are not limited to the following:

- Requirement for barrier system type - will it be used to guide pedestrian and vehicle flow or to preclude vehicle intrusion into a restricted zone or area?
- Installation plans - heavy equipment is usually needed for the placement of temporary barriers, while excavation and/or construction is usually required for permanent installation of larger systems
- Required number and placement - how many of the barrier system units will be required and how will they be arranged or spaced?
- Aesthetic requirements for barrier system - are special styles, shapes, sizes, colors, or textures required?
- Local codes - may require or preclude certain types of barrier systems

3.3 LIGHTING SYSTEMS

3.3.1 Technology

Lighting systems are installed to provide illumination of protected areas. This illumination increases the sensitivity of intrusion detection surveillance by technology and personnel. In addition, lighting provides deterrence to intruders by shedding light on suspicious activity and helps prevent covert access to restricted and protected areas.

Tables 11 and 12 provide a reference to available technologies and systems. Columns are as follows:

- Lighting System – A list of the types of lighting systems available
- System Description – A short description of the lighting system
- System Utilization – The application of the lighting system
- Systems Strengths – Positive attributes of the lighting system
- System Weaknesses – Negative attributes of the lighting system

Table 11 - Lighting Systems

Lighting Systems	System Description	System Utilization
Incandescent	Oldest most common light source. Light emitted from current flow through tungsten filament. Current heats filament to produce visible light	General Lighting
Tungsten Halogen	New type of incandescent with gas filled bulb and inner coating to reflect heat. Reflected heat increases efficiency	Commercial, highlighting
Reflector Lamps	Incandescent lights with reflectors to focus light in desired patterns	Flood lighting, spot lights, down lighting - parabolic and ellipsoidal
Fluorescent	"Tube" lights, mercury and inert gas in tube is energized to produce UV light, UV light strikes phosphor on tube interior to emit visible light	Work space and area lighting
Compact Fluorescent	Fluorescent "Bulb" light design into standard bulb shape	Design as direct replacement to incandescent lights
Solid State Light Emitting Diode (LED)	Solid State semiconductor device that emits various color lights with current flow	Replacement for incandescent lighting, currently mostly used for panel lighting and traffic lights
Solid State Infrared (IR) LED	Solid State semiconductor device that emits various color lights with current flow	Provide IR illumination for CCTV systems
High Intensity Discharge (HID)	Light technology including Mercury Vapor, Metal Halide, and High Pressure Sodium, high intensity discharge between two electrodes creates light	Street lights, gyms, area lighting, security lighting
Mercury Vapor	Uses mercury vapor as conductor	Street lights, gyms, area lighting
Metal Halide	Metal Halide conductor	Street lights, stadiums, area lighting, security lighting
High Pressure Sodium	High pressure sodium conductor	Street lights, stadiums, area lighting, security lighting
Low Pressure Sodium	Similar to fluorescent lights with low pressure sodium	Highway & Security Lighting
Sulfur	New Product - Sulfur enclosed in sealed bulb bombarded with microwave energy	Area, work areas, security lighting

Table 12 - Lighting Systems Strengths and Weaknesses

Lighting Systems	System Strengths	System Weaknesses
Standard Incandescent	Inexpensive to buy, readily available, instant on, easy to replace, warm color	Very inefficient 20 or less lumens per watt, short life span 800 hours, runs very hot, long life bulb (thicker filaments) are even lower efficiencies, Not shock or vibration resistant
Tungsten Halogen	Desirable color renditions, more efficient that standard incandescent, instant on, warm color	Considerably more expensive than standard incandescent, lower efficiencies than other lighting
Reflector Lamps	Inexpensive and readily available, instant on, easy to replace, warm color, increase efficiency by "focus" of available light	Incandescent - high heat, inefficient, short lifetime
Fluorescent	3 to 4 time as efficient (75 lumen per watt) as incandescent lighting, 10 time longer life (10,000 hours)	Delayed start up, require ballast to operate, contain toxic chemicals (mercury & phosphor), cool light, potential cold weather performance problems
Compact Fluorescent	Same as Fluorescent (Higher efficiency and longer life) with ability to replace Incandescent, integrated ballast	Same as Fluorescent, 10 times the cost of incandescent bulb replaced
Solid State Light Emitting Diode (LED)	Extra Long life (100,000 hours), efficient (25 lumens per watt - dependant on color), runs cool, instant on, available in all viable colors, very shock resistant	Expensive (100 times Incandescent), not available in high light output, whites and blue color higher cost than standard red
Solid State Infrared (IR) LED	Invisible to naked eye, efficient, run cool, instant on	Expensive, low light out, large matrix of LED required for flood or zone lighting
High Intensity Discharge (HID)	Save 75 to 90 lumens per watt energy consumption compared to incandescent	Not instant on, restart /start time may pose security problem
Mercury Vapor	50 lumens per watt, 24,000 hour life	Older technology now replaced by metal halide or high pressure sodium, very cool blue / green light, very slow start up
Metal Halide	Better color than Mercury Vapor, 75 lumens per watt, good for CCTV color	Slow start up and restart after power failure
High Pressure Sodium	90 lumens per watt, 24,000 hour life	Slow start up and restart after power failure
Low Pressure Sodium	Very efficient (100 lumens per watt), long life (16,000 hours)	Poor yellow / gray light color, poor CCTV color rendition
Sulfur	Very Efficient (over 100 lumens per watt), long life 60,000 hours (no filament)	New technology not widely available, currently used in experimental locations, not available in low output sizes

3.3.2 Applications

Lighting technologies provide a means for application of lighting. Table 13 provides insight into different applications of lighting and follows the same description, utilization, strengths, and weaknesses format of the technology tables.

Table 13 - Lighting System Applications

Type of Lighting	Recommended Lighting Systems	System Description	System Utilization	System Strengths	System Weaknesses
Lighting Applications					
Wide-Area Lighting	Metal Halide Sodium (High & Low Pressure) Sulfur	Designed to provide lighting to a wide area of coverage	Large parking areas, fields, long lengths of roads, streets, or highways	Provides non-intrusive "general" lighting over a very large area, low cost	Some lighting "bleed-over" into areas that may not need or desire lighting
Spot / Zone Lighting	Standard Incandescent Tungsten Halogen Reflector Lamps Fluorescent	Designed to provide lighting to a specific area or zone	Security gate areas or zones around high-value assets	Provides dedicated lighting for special requirements, low cost	If not properly used, could be used by threat concern to identify high value areas
Mobile Lighting	Standard Incandescent Tungsten Halogen Reflector Lamps LED Fluorescent	Transportable design to provide lighting to areas where needed and when needed	Temporary work-sites, temporary security gates or security checkpoints	Provides substantial lighting at remote or non-powered sites for extended periods	Usually trailer-mounted and generator powered. Must be moved with vehicle
CCTV Illumination	Standard Incandescent Tungsten Halogen Reflector Lamps IR LED Metal Halide	Designed specifically to provide support lighting for use of closed-circuit camera systems	Surveillance camera fields of view (IR lighting for "no light" or "blackout" conditions")	Provides lighting in lowest-light ("no-light") conditions	Specialized lighting, IR lighting can be seen with special detection equipment
High-Intensity Spot Lighting (fixed)	Incandescent Tungsten Halogen Reflector Lamps	Designed to provide high-intensity lighting for a specific area or zone ("spot")	Bridges, guard towers, security gates	Very powerful and controllable lighting to meet emergency spot-lighting requirements	May need mounting atop buildings, gates or guard towers, higher cost
High-Intensity Spot Lighting (hand-held)	Tungsten Halogen	Designed to provide hand-held high-intensity lighting beyond that of a typical "flashlight"	Security personnel, vehicles, vessels or first-responders	Very portable, up to 6-million candlepower, 1-to-40-degree adjustable beam-width, debilitating strobe light feature	Requires carrying a belt-mounted rechargeable battery pack. Can be damaged if not properly handled or used

3.3.3 Costs

Lighting System characteristics are only part of the information required to choose an appropriate system. In addition, implementation, maintenance, training, and life expectancy must be included in the selection criteria. The following table provides a summary of costs. Please note that even though materials costs are similar throughout the US, labor costs vary as much as 3 times and this will affect the amounts shown in the tables. In addition, electric rates vary by a factor of 3 times. Each authority will need to include these factors in implementation and support of the deployed systems.

Table 14 provides a reference to rough systems costs.

- Lighting System – A list of the types of lighting system
- Cost of Implementation – Rough range of installing system
- Cost of Maintenance – including operational costs expressed as a yearly % of implementation
- Cost of Training – extra or special training expressed as a one time % of implementation
- Life Expectancy – System life expectancy in years

Table 14 - Lighting Technologies Cost Matrix

System	Rough Cost of Implementation	Comments	Cost of Maintenance & Operation % per year	Comments	Cost of Training % one time	Comments	Life Expectancy
Standard Incandescent	$100 to $1K per fixture	Inexpensive and easy to install, labor largest part of cost	40-50%	Very high costs for electric power. Inexpensive Lamps & easy to replace	0	No training, Standard Electrician can maintain system	Infrastructure 20+ years. Lamp - 800 hours
Tungsten Halogen	$100 to $1K per fixture	Installation the same as Incandescent with 10-20X Lamp cost	35-45%	Specialty lighting normally not for security	0	No training, Standard Electrician can maintain system	Infrastructure 20 to 25 years. Light Lamp - 2-10K hours
Reflector Lamps	$100 to $1K per fixture	Addition of reflector to Incandescent	40-50%	Same as incandescent	0	No training, Standard Electrician can maintain system	Infrastructure 20+ years. Lamp - 800 hours
Fluorescent	$100 to $1K per fixture	Location & temperature contribute to wide cost variations	10-30%	Ballast may need replacement before end of system life	0	No training, Standard Electrician can maintain system	Infrastructure 20+ years. Lamp - 10K hours
Compact Fluorescent	$6 to $15 a lamp	Normally used to replace incandescent lamps	15-35%	Ballast replaced with "Lamp"	0	No training, Standard Electrician can maintain system	Infrastructure 20+ years. Lamp - 10K hours
Solid State Light Emitting Diode (LED)	$100 & up - low watts $20 & up	Replacement for incandescent lamps	15-35%	Electrical and Cleaning costs only, excellent for difficult access area	0	No training, Standard Electrician can maintain system	Infrastructure 20+ years. Lamp - 100K hours
Solid State Infrared (IR) LED	$350 for system, $100 & up for mounting	Provide "invisible" illumination for cameras	15-35%	Electrical and Cleaning costs only	25	Need education on "invisible" light system and test unit	Infrastructure 20+ years. Lamp - 100K hours
Mercury Vapor	-	Obsolete System / Technology for new systems	-	-	0	No training, Standard Electrician can maintain system	Infrastructure 20+ years. Lamp - 24K hours
Metal Halide	$1-5K per fixture	Cost vary widely by system size & utility work required	15-25%	Electrical costs & lamp replacement 1 to 3 years	0	No training, Standard Electrician can maintain system	Infrastructure 20+ years. Lamp - 12-24K hours
High Pressure Sodium	$1-5K per fixture	Cost vary widely by system size & utility work required	15-25%	Electrical costs & lamp replacement 1 to 3 years	0	No training, Standard Electrician can maintain system	Infrastructure 20+ years. Lamp - 24K hours
Low Pressure Sodium	$1-5K per fixture	Cost vary widely by system size & utility work required	10-20%	Electrical costs & lamps replacement 1 to 3 years	0	No training, Standard Electrician can maintain system	Infrastructure 20+ years. Lamp - 16K hours
Sulfur	$100K-300K per installation	Experimental System for large areas	-	Experimental System	1	No training, Standard Electrician can maintain system	Infrastructure 20+ years. Lamp - 60K hours

3.3.4 Other Factors

There are other factors that must also be considered in the implementation of a lighting system. These include, but are not limited to the following:

- Power supply and power supply reliability
- Lamp re-strike and warm up time in the event of loss of power (see Table 15)
- Coordination of design with Video System
- Light pollution – some locations and neighborhoods may object to security lighting and to illumination of adjacent areas
- Light spectrum – some location may object to the light spectrum of the chosen solution (objections to the 'color' of the lighting)
- Environmental – some locations require use of certain lighting types for increased energy efficiency; this may contribute to poor performance for CCTV applications
- Visible versus Invisible lighting – visible lighting provides a deterrence to intrusion, but some applications and operational requirements may require covert lighting

Table 15- Lamp Re-strike Times

Lamp Type	Re-strike Time
Incandescent	Real Time
Tungsten halogen	Real Time
Mercury Vapor	3 to 7 minutes
Fluorescent	Sub minute
Metal Halide	Up to 15 minutes
High Pressure Sodium	1 minute re-strike, 3 to 4 minute warm up
Low Pressure Sodium	7 to 15 minutes

3.4 VIDEO SYSTEMS

3.4.1 Technology

Video systems provide a method to remotely monitor and assess security areas. Application of a video system is part of the overall design of the IDS. System vendors and technical expertise can provide additional and equipment specific application data. In addition, TCRP has published a report on transit video surveillance (*TCRP Synthesis 38: Electronic Surveillance Technology on Transit Vehicles)* that can provide information on the more complex issues of storing/archiving video data and transmitting it to another location (this information is outside of the scope of this Handbook). Some generic guidelines are provided here to help focus the application of the technologies that are described in the next section.

- For new installations, Lighting and Video Systems should be designed concurrently
- For existing lighting, the Video Systems can be designed to existing lighting or lighting can be updated

- Visible versus invisible – an assessment of what lighting is available and deployable will help determine the type of video imaging systems. Some factors include stealth and light effects on neighbors.
- Unless stealth is desired, a minimum illumination of 2 foot-candles throughout assessment area should be maintained. Avoid high contrast ratios to prevent video blooming.
- Cameras are primarily used to assess IDS zone and can be one camera per zone, one camera per many zones, and, in some instances, multiple cameras per single zone. If costs allow, all IDS zones should have video assessment available and automatically be called up (activated) upon alarm. This allows quick assessment and response to IDS alarms.
- Set field of view (FOV) by optimal selection of camera image format size, lens focal length, and zoom setting if applicable
- Use lens, zoom, and terrain conditions when setting and selecting camera locations
- Be aware of rising and setting sun when setting camera alignment
- Mount cameras at safe height to prevent damage and provide good field of view. Also if possible, mount cameras inside secure areas and provide tamper protection if the camera is subject to tamper.
- Firm mounting masts are required to prevent motion by wind or pan / tilt unit movement. This is particularly important for higher power lens used for looking longer distances.
- Provide appropriate camera housings for worst-case environmental conditions – outdoor, cold, hazardous conditions, etc.

3.4.2 Applications

Video systems are installed to provide visual assessment of protected areas and thus improve security. In conjunction with proper lighting, video systems provide deterrence to intruders by allowing viewing of suspicious activities and increase security force efficiency by allowing quick assessment of intrusion alarms. An added capability is the recording of video signals that can aid in post incident analysis and legal action.

Tables 16 - 19 provides a summary of available technologies and systems. Columns are as follows:

- Video Systems – A list of the types of video systems and equipment available
- System Description – A short description of the video system
- System Utilization – The application of the system
- Systems Strengths – Positive attributes of the system
- System Weaknesses – Negative attributes of the system

Table 16- Video Systems – Imaging Devices and Imaging Control

Video Systems/Components	System Description	System Utilization
Imaging Devices		
Monochrome (Black & White)	Monochromatic image collection device that converts photons to electronics	Functions as retina of camera system
Tube	Imaging tube is used to convert scene light into an electronic signal	Light image to electronic signal converter
Solid State	Solid state image devices convert photon to electrons - CCD charged coupled device, CMOS complementary metal oxide semiconductors and others	Light image to electronic signal converter
Color	Color image collection device that convert photon to electrons in 3 color bands - Red, Green, Blue	Retina of camera system
Tube	Imaging tube is used to convert scene light into an electronic signal	Light image to electronic signal converter
Solid State	Solid state image devices convert photon to electrons - CCD charged coupled device, CMOS complementary metal oxide semiconductors and others	Light image to electronic signal converter
Convertible	Color Image at higher light levels (about 1 lux) and Black & White at lower	Color at high light level, Black & White at low
Thermal Imaging System (TIS) Camera	Imaging system that convert Infrared Light (IR) photons to electronic signal, Visible Light is about 0.4 to 0.7 microns, Near IR is 0.7 to 3.0, Mid Wave IR is 3.0 to 6.0, Long Wave IR is 6.0 to 15, and Very Long Wave IR is about 15. Imaging sensors examples include InGaAs (indium gallium arsenide, InSb (indium Antimonide), Microbolometer and QWIP (quantum well infrared photo detectors)	Uses emission of IR photons not reflection of visible photons
Lens	Optical device to collect and direct light to imaging device - eye of camera	Used to set field of view and light collection ability
Imaging Control		
Zoom Lens	Optically or Digital controllable zoom features	Used to zoom in on video scene of interest
Optical	-	-
Digital	-	-
Pan and Tilt	Controllable camera mount that allow Pan (side to side motion) and Tilt (up and down motion) of camera	Used to aim camera at desired view point, can be manual or automated control
Iris Control	Control to allow amount of light onto image sensor	Extreme light conditions, Iris control is normally an automatic function controlled by lens or camera imager
Focus Control	Manual method to focus lens view	Adjust for change lens focus
Image Intensifiers	Device that electronically amplifies available light	Extra low light conditions
Security Mirrors	Optical Reflective Mirrors	Allow camera to see around blocking objects
Wiper / Washer System	Wiper / Washer similar to car windshield device	Use to clean and clear objects off of camera enclosure window
Heater / Cooler	System to heat or cool camera enclosure	Maintain camera system within operational temperature ranges

Table 17 - Video Systems Strengths and Weaknesses – Imaging Devices and Imaging Control

Video Systems	System Strengths	System Weaknesses
Imaging Devices		
Monochrome (Black & White)	More sensitive in low light levels than color cameras	No color image to help identify image under view
Tube	Excellent image quality in new system	Obsolete technology (40 years old), image burn in, short tube life, requires 10 lux illumination, smear and flare problems
Solid State	Current Technology, some models work in 0.1 lux or less, high resolution	Proper selection requires detailed knowledge of lens characteristics and capabilities, no color to aid in identification
Color	Provides color images	Less sensitive to low light illumination, more complex and expensive than Black & White cameras
Tube	Excellent image quality in new system	Obsolete technology (40 years old), image burn in, short tube life, requires 40 to 100 lux illumination, smear and flare problems
Solid State	Current Technology	Proper selection requires detailed knowledge of lens characteristics and capabilities, need more light than black & white system
Convertible	Provide best of both Black & White and Color	Expense, lower resolution than Black & White camera
Thermal Imaging System (TIS) Camera	Require no ambient light, can covertly view areas, NIR can be supplemented with IR spot lights, prices are dropping and capabilities increasing	Expensive, need IR source to view, lower quality and resolution, monochromatic images (false color available), higher maintenance cost, some systems require expensive cooling systems, Proper selection requires detailed knowledge of characteristics and capabilities
Lens	Numerous versions and models available for different format imagers, focal length, f-stop, optical quality, filters, mount type, and control (see below)	Proper selection requires detailed knowledge of lens characteristics and capabilities, special expensive lens required for IR imaging devices
Imaging Control		
Zoom Lens	-	-
Optical	Allow large zooms without loss of picture quality	Expensive, larger lens size, larger zooms are very expensive and require robust and stable mounting
Digital	Inexpensive software adaptation	Zoom degrades picture quality, only available on certain models of camera systems
Pan and Tilt	Allows one camera to cover larger area, allows camera to be directed to area of interest	Expensive, must maintain system, must provide interface control and data link
Iris Control	Allow precise control on light	Requires manual control system, automatic control sufficient for most systems
Focus Control	Provide manual control for fine adjustment and zoom systems	Manual control, properly adjusted fixed system doesn't require this feature, properly adjusted zoom systems requires minimal control
Image Intensifiers	Allows viewing in extra low light conditions	Expensive, Image problems with large view contrast, requires non standard controller, difficult to adjust, not needed for well-lit areas or with IR cameras
Security Mirrors	Inexpensive, allows single camera to see "around" corners	Limited resolution and low quality of view, requires pan/tilt/zoom camera for full utilization
Wiper / Washer System	Allows remote wipe / wash of enclosure window	Require extra control, maintenance, washer refill (with non freezing solution)
Heater / Cooler	Allow camera system operation in harsh temperature environments	Expensive (for cooler), required added power, system maintenance

Table 18 - Video Systems – Data and Power Transmission, Viewing Devices, Video Control Devices, Video Recording Devices

Video Systems	System Description	System Utilization
Data and Power Transmission		
Camera Power	Power supply for camera, lens, pan, tilt, image intensifier, wipe, wash, etc.	Use to power camera systems
DC	DC powered system	Used for camera and zoom
AC	AC line power system	Used for complete systems
Solar / Stand Alone	Solar Powered	Used were power is not readily available
Control Signals	Methods to send control signal to camera system	Zoom, Pan, Tilt, Image intensifier, wipe, wash, etc.
Wire	Metallic cable with insulation	-
Fiber Optic	Glass Fiber Optic cable with protective outer jacket	-
RF	Radio Frequency Wave	-
Video Signals	Method to send video from camera to viewing and control devices	Viewing of video signal
Wire	Metallic cable with insulation, normally RG-59, 6, or 11: 75 ohm coaxial cable, can be twisted pair with driver converter	-
Fiber Optic	Glass Fiber Optic cable with protective outer jacket, plastic fiber optic used is special short run classified locations	-
RF	Radio Frequency Wave	-
Viewing Devices		
Video Monitors CRT	Allow viewing of video signal	Observation of video images
Video Monitor Flat Panel	Allow viewing of video signal, Including LCD, Plasma, Field Emission	Observation of video images
Video Control Devices		
Pan / Tilt / Zoom Control	Control system that allow pan/tilt/zoom manipulation	Steer camera image to desire location
Iris Control	Control system to open lens iris to allow more or less light onto camera imaging device	Adjust amount of light input to form video image
Focus Control	Control system to adjust lens focus	Change lens focus when scene changes
Image Intensifier Control	Electronics device to amplify available light	Allows viewing of low light scenes
Video Switcher	Switcher to route video signals from multiple cameras to lower number of monitors	Human interfaces design dictates a limited number of monitors to provide effective viewing, video switcher provide a higher number of video signals to lower number of viewing monitors
Video Matrix Switcher	An electronic switching system that allows support for a large number of cameras, monitors and recording devices. Enable intelligent control and viewing of video systems	Control and monitoring of medium to large video surveillance systems
Video Recording Devices		
Video Tape Recorder	Recording of video signal on magnetic tape - Video Cassette Recorder VCR	Archive of video for review, legal, and security requirements
Digital Video Recorders (DVR)	Recording of video signal on computer hard disk	Archive of video for review, legal, and security requirements
DVR Control System	Control system and interface for DVR	Controls of a system of numerous DVRs

Table 19 - Video Systems Strengths and Weaknesses – Data and Power Transmission, Viewing Devices, Video Control Devices, Video Recording Devices

Video Systems	System Strengths	System Weaknesses
Data and Power Transmission		
Camera Power	Necessary	Must provide reliable and stable power, poor power means poor quality
DC	Stable and quality power easily provided, simple battery back up	Voltage drop problems for long distance from supply to camera system, not suitable for larger system loads such as large pan / tilt units, must run power to camera system
AC	Large power loads easily accommodated	Stability and quality problems, complex power back up, must run power to camera system
Solar / Stand Alone	Provides power where normal supplies are not available, self contained	Requires sunlight input, High costs, battery maintenance, limited load capability
Control Signals	Required for operation	More complex than automated control (when available)
Wire	Inexpensive, easy to connect and install	Limited to shorter distances, subject to electro magnetic interference
Fiber Optic	Immune to EMI, allows long distance connections, interface from wire control to extend control distance	Expensive, requires special tools for installation and connection, Requires electric to optical conversion equipment
RF	No wire or fiber required	Expensive, subject to EMI interference, not secure, in higher frequency systems limited to line of sight only
Video Signals	Required for operations	-
Wire	Inexpensive, easy to connect and install	Limited to shorter distances (1,000 feet for RG-11), subject to electro magnetic interference and ground loops
Fiber Optic	Immune to EMI, allow long distance (more than 50 miles) connections	Expensive, requires special tools for installation and connection, Requires electric to optical conversion equipment, plastic limited to about 100 feet
RF	No wire or fiber required	Expensive, subject to EMI interference, not secure, mostly limited to line of sight connection
Viewing Devices		
Video Monitors CRT	Industry standard	Monitor burn in (from viewing same unchanging image), System aging contributes to loss of image quality, large depth, heat output
Video Monitor Flat Panel	Thin, lower power consumption, limited image degradation over time	Expensive, need Video-to-monitor adapter / driver
Video Control Devices		
Pan / Tilt / Zoom Control	Allow precise manual control	More complex system to install and maintain
Iris Control	Allow precise manual control	Normally automatic control is sufficient, added user control point with accompanying system, training, and maintenance
Focus Control	Allow precise manual control	None - required feature
Image Intensifier Control	Allow viewing of video image where normally none would be seen, provides manual control	Non standard control and not available on all control systems
Video Switcher	Inexpensive, simple to install and operate	Does not provide advanced features of a matrix switcher (see below), supports only small and limited number of video signals and monitors
Video Matrix Switcher	Allows assignment of many cameras to manageable number of monitors, includes provisions for control, routing to video recorder devices, interface to and from ACS and IDS, automatic control of pan / tilt / zoom and other camera control functions, allow loss of video and other alarms	Expensive, complex to install and configure, more difficult operation, training required
Video Recording Devices		
Video Tape Recorder	Inexpensive, easy to operate, tapes easily transported	Medium to low video quality, difficult to archive and save tapes, difficult to find required video information, loss of video tapes, storage of video tape, maintenance of VCRs
Digital Video Recorders (DVR)	Drop in replacement of VCR, higher image quality available, easier and quicker access to video scenes, can be downloaded to CD-ROM/floppy drive, incidents can be downloaded from a remote site using client software	Expensive, must support, back up, and maintain DVR computer system, requires compression of video for effective operation, large hard disk required, digital video files are very large
DVR Control System	Allows network access and control to DVRs	Complex computer system, requires back support, and training

3.4.3 Costs

Video system characteristics are only part of the information required to choose an appropriate system. In addition implementation, maintenance, training, and life expectancy must be included in the selection criteria.

The following tables provide a summary of costs. Please note that even though materials costs and similar throughout the US, labor costs vary as much as 3 times and this will affect the amounts shown in the tables. Each authority will need to include this factor in implementation and support of the deployed systems.

Tables 20 – 22 provide a reference to rough systems costs.

- Video Systems – A list of the types of video system
- Cost of Implementation – Rough range of installing system
- Cost of Maintenance – including operational costs expressed as a yearly % of implementation
- Cost of Training – extra or special training expressed as a one time % of implementation
- Life Expectancy – System life expectancy in years

Table 20 - Video Systems Cost – Camera Systems and Image Control

System	Rough Cost of Implementation	Comments	Cost of Maintenance & Operation % Per year	Comments	Cost of Training % one time	Comments	Life Expectancy
Camera Systems							
Monochrome (Black & White)	-	-	-	-	-	-	-
Tube	-	Obsolete	-	-	-	-	1 to 2 years for image tube
Solid State	$100 to $1K	In some instances installation and infrastructure costs exceed camera costs	5%	Little to no maintenance	0% -5%	Little to no training required	5 to 7 years
Color	-	-	-	-	-	-	-
Tube	-	Obsolete	-	-	-	-	1 to 2 years for image tube
Solid State	$500 to $3K	In some instances installation and infrastructure costs exceed camera costs	5%	Little to no maintenance	0% -5%	Little to no training required	5 to 7 years
Convertible	10% to 20%	Small premium on color camera	5%	Similar to color	0% -5%	Little to no training required	6 to 7 years
Thermal Imaging System (TIS) Camera	$10 to $200K	Very WIDE range of capabilities and costs. Factors - image resolution & cooling	10%	Most units are sealed, cooling system and imager maintenance dependant on use hours	10%	For higher end systems, low end systems are similar to standard video	3 to 5 years, can be refurbished for extend life
Imaging Control							
Zoom Lens	-	-	-	-	-	-	-
Optical	$40 to $5K	Fixed versus zoom, F stop, mm size, auto iris, auto focus, etc.	<5%	Cleaning	0%	None	Life of camera
Digital	10%	Included in the cost of some imaging camera systems, small to no premium	0%	No maintenance, part of camera system	0%	None	Life of camera
Pan and Tilt	$1K to $3K	Cost varies according to load and speed, some systems include integral pan & tilt (dome cameras)	5%	Cleaning and lubrication	5%	Minimal training for maintenance procedures	5 to 10 years
Iris Control	$0	Include in most lens	<5%	Normally no maintenance	0%	None	Life of camera
Focus Control	$0	Include in most lens	<5%	May need adjustment	0%	None	Life of camera
Image Intensifiers	$15 to $30K	Add on between lens and camera system	Varies	Imager tube can be damaged by excess light, life expectancy 10K hours	5%	Minimal training for maintenance procedures	10,000 hours for tube, system 5+ years
Security Mirrors	$20 to $100	Available in various shapes and materials	<5%	Routine cleaning	0%	It is a mirror	10+ years
Wiper / Washer System		Addition to outdoor camera systems		Keeping washer fluid tank filled is problematic. Wiper blades and fluid hose need frequent replacement	5%	Minimal training for maintenance procedures	System 5 to 10 years, wiper blades & hoses 1 to 3 years
Heater / Cooler	$5 to $500	Heater simple resistive add on, cooler are expensive	5% - 20%	Electrical power and AC maintenance	0%	None for heater, Cooler is standard AC system	Heater life of camera housing, Cooler 5 - 10 years

Table 21 - Video Systems Cost – Data and Power Transmission, Viewing Devices

System	Rough Cost of Implementation	Comments	Cost of Maintenance & Operation % Per year	Comments	Cost of Training % one time	Comments	Life Expectancy
Data and Power Transmission							
Camera Power	-	-	-	-	-	-	-
DC	$100 to $350	Small AC to DC power supply with battery	5%	Battery replacement every 3 to 5 years	0%	None	10+ years
AC	$20+	AC transformer	<5%	No maintenance	0%	None	10+ years
Solar / Stand Alone	$500 to $2K	Solar Panel with power conditioner and battery back up, dependant on power consumption and available sun light	10%	Clean solar panels & Battery replacement every 1 to 3 years	5%	Cleaning & set up procedures	5 to 7 years
Control Signals	-	-	-	-	-	-	-
Wire	50 cents to $3 per foot	Control wires from control station to camera unit	<5%	Little to no maintenance	<5%	Training on camera control	10+ years
Fiber Optic	Cable $1+ per foot, Converters $500 to $2K each	Can use same equipment and multiplex signal	<5%	Little to no maintenance	25%	Training on fiber optics methods, testing, maintenance, and safety	10+ years
RF	Add $0 to $5K	Required return channel from control station to camera, included in some RF video units	10%	Routing antenna alignment, cleaning and frequency check	20%	RF and video set up and maintenance	5 to 10 years
Video **Signals**	-	-	-	-	-	-	-
Wire	Coax Cable $0.50 foot and up, converters $250 and up	Coax or twisted pair with converter, dependant on distance	5%	Little to no maintenance, converters may need adjustment	10%	Training on testing of video signals	10+ years
Fiber Optic	Cable $1+ per foot, Converters $500 to $2K each	Require electro-optic converters, highly dependant on distance	<5%	Little to no maintenance	25%	Training on fiber optics methods, testing, maintenance and safety	10+ years
RF	$2K to $50K	Radio link dependant on frequency, distance, and line of sight	10%	Routing antenna alignment, cleaning and frequency check	20%	RF and video set up and maintenance	5 to 10 years
Viewing Devices							
Video Monitors CRT	$150 to $500	Cost dependant on resolution and screen size	20%	Low maintenance, some monitors may experience 'burn in' from fixed images	5%	Cleaning procedures & calibration	5 to 7 years
Video Monitor Flat Panel	$350 to $20K	Cost dependant on screen size, need converter for some panels, extra large sizes available	10%	Low maintenance, lower power consumption, and lower heat output compared to CRT	<5%	Special Cleaning	5 to 10 years

Table 22 – Video Systems Cost – Video Control Devices, Video Recording Devices

System	Rough Cost of Implementation	Comments	Cost of Maintenance & Operation % Per year	Comments	Cost of Training % one time	Comments	Life Expectancy
Video Control Devices							
Pan / Tilt / Zoom, Focus & Iris Control	$500 to $2K	Normally keyboard / joy stick device, many include video switcher, can be software controlled via computer and RS-232 /422 interface	<5%	Routine cleaning	10% to 20%	Some systems are counterintuitive and difficult to operation	5 to 10 years
Image Intensifier Control	$1 to $3k	Control System for Image Intensifier, typically RS-232 computer control	10%	Low maintenance computer control	<5%	Operation training	5 to 10 years
Video Switcher	$100 to $3K	Simple low end switch of video signals to monitor & recording devices, dependant on channels and automatic features	<5%	Little to no maintenance, no to very low power consumption	<5%	Normally simple push button operation	10+ years
Video Matrix Switcher	$5K and up	Large cost variation on number of video inputs and outputs. Ranges as high as 2,000+ inputs	<5%	Low maintenance	10%	Operational training and support	10+ years
Video Recording Devices							
Video Tape Recorder	$250 to $1K	Standard Security VHS Tape Recorder, home unit not acceptable, features determine cost	20%	Video heads must be clean, and tape archived, rotated, and replaced	0%	It is a VCR!	3 to 5 years depending on use
Digital Video Recorders (DVR)	$2k to $10K	Dependant on software features and hard disk space	<10%	Low maintenance self contained unit, low power consumption	10%	Similar to VCR control, also need computer interface and back methods	5 to 7 years
DVR Control System	$10K to $50K and up	Integrated Computer Control System, cost depend on size and complexity including network distribution and control	20%	Complex computer system with large amount of disk storage and recorded video back system, high bandwidth demands on network	25% and up	Training in network operation & support	5 to 7 years, may need to replace failed hard disks

3.4.4 Other Factors

There are other factors that must also be considered in the implementation of video systems. These include, but are not limited to the following.

- Coordination with Lighting System installation
- Privacy concerns of viewing and recording video images
- Work rule concerns of viewing and recording video images
- Legal implications of video surveillance
- A system for archiving recorded video must be established and supported. This includes, but is not limited to the following:
  - Legal requirement
  - Chain of custody
  - Storage medium selection
  - Secure and temperature controlled storage area
  - A method to retrieve and return archived video

3.5 ACCESS CONTROL SYSTEMS

3.5.1 Technology

Access control systems provide a method to control through a credential or token the entry and, if desired, the exit from a controlled secure area. The control method can be anything from a key, to access card, to a biometrics data file. The form and method of selection is determined by the transit system's requirements, budget, and technology growth path.

Besides providing positive control of personnel movement, the ACS, when interfaced to the IDS, provides a method to both suppress and enable alarms. The ACS provides control to the IDS by either time/date or via individual access grants. The proper integration of this feature provides an orders-of-magnitude increase in system function.

Currently there are no ACS requirements or standards for transit facilities, but examples and standards can be found in other industries and transit areas. ACS vendors provide features and functions that have developed over years of fulfilling commercial requests and requirements. These vendor 'features and functions' can be taken as commercial standards since currently there are no mandated standards for private industry. An excellent example of non-military systems is published by the FAA (107.14 for ACS at United States airport facilities). Military standards can be found in various military handbooks.

Chapter 4 contains a survey list used to quantify and qualify the ACS. A short summary is included here.

- Determine the number and locations of access systems required
- If multiple locations are required ensure there is network connectivity
- Identify the number of access 'portals' (controlled gates and doors) for each security zone
- Determine access rules by personnel and time

- Determine what needs to be tracked – people and materials
- Determine the number of badges required
- Determine if there are hazardous conditions
- Is a physical characteristic for an individual required for positive identification (a biometric such as fingerprint or retinal scan)?
- What type of reader and badge is required?
- Determine badge layout and numbers required
- Determine data history and requirements
- Determine any integration with other systems, e.g.,
    - IDS
    - Video
    - HR
    - Attendance

3.5.2 Applications

Access control systems technologies cover the spectrum from simple keys to highly integrated biometrics controls. Tables 23 – 26 provide a summary of the systems. Note that in addition to the benefits listed above an ACS can also provide historical access data that can aid in post-incident analysis and potential legal action. Columns are as follows:

- Access Control Systems – A list of the types of systems and equipment available
- System Description – A short description of the systems and equipment
- System Utilization – The application of the system
- Systems Strengths – Positive attributes of the system
- System Weaknesses – Negative attributes of the system

Table 23 - Access Control Systems - Credentials

Access Control Systems	System Description	System Utilization
Credentials		
Mechanical Key	Standard and custom metal key used to open mechanical locks	Provide controlled access to locked areas and facilities
Mechanical Combination	Combination Mechanical Locking	Locking of doors and cabinets
Electronic Combination - Key Pad	Electronic version of combination lock. Uses numeric or alpha numeric keypad	Locking of doors and cabinets
Electronic Credential	A device with memory that is used to enable access to an electronic control system, Magnetic Stripe, Wiegand, Proximity, Laser Card, Barcode, Smart Card. Stored information used by access control system to validate and control access.	Access to controlled and security areas, audit of access, database tracking
Barcode	A one or two dimension printed code, similar to UPC on food items	Tracking of cards and products
Magnetic Stripe	Magnetic material applied to card, best example credit cards	Access control and financial transactions
Wiegand	Short length of heat treated wire installed in plastic card, external magnetic field energizes card to allow reading of code	Access control
Proximity	RF embedded antenna inside card, RF signal from reader activates and collects data from card	Non contact read and authorization of credential
Smart Card	Memory chip installed in card contains data and computer processor	Storage of user data, cryptographic and security processing
Proximity Smart Card	Memory chip installed in card contains data and computer processor, interface via proximity	Storage of user data, cryptographic and security processing
Other Cards	Magnetic Spots, Optical Storage, IR barcode, etc.	Access control
Biometric Credential	Use human biometric characteristic to identify user, Fundamental criteria - Failure to enroll, False Acceptance Rate, False Rejection Rate, and ergonomics/ease of use	User verification and authentication
Finger Print - Optical	Optical scanner measures finger print	Finger print image - location & direction of ridge endings and bifurcations
Finger Print - Capacitive	Capacitive sensor measures finger print	Finger print image - location & direction of ridge endings and bifurcations
Finger Print - Ultrasonic	Ultrasonic sound wave measures finger print	Finger print image - location & direction of ridge endings and bifurcations
Iris Scan	Optical scanner measures iris	Iris image - furrows & striations on iris
Retinal Scan	Optical scanner measures eye retinal pattern	Retina image - blood vessel pattern
Hand Geometry	Optical 3D measure of hand shape	3D image of hand - height & width of bones & joints of hands & fingers
Face Scan	Electronic imaging (Camera or IR camera) device measure facial characteristics	Facial image - relative position & shape of nose, position of cheekbones
Voice Print	Voice "signature" via spoken input	Voice recording - frequency, cadence, & duration
Signature	Electronic version of signature via electronic stylus and input pad	Signature image and writing dynamics
Other Methods	Bone structure, body thermal imaging, hand blood vessel pattern, etc.	-

Table 24 - Access Control Systems – Credentials Strengths and Weaknesses

Access Control Systems	System Strengths	System Weaknesses
Credentials		
Mechanical Key	Inexpensive, no electrical power required, established infrastructure, easy to duplicate and distribute keys	Key inventory control very difficult, loss of key requires lock replacement, Locks can be picked, unauthorized key duplication
Mechanical Combination	Combination can be changed, no electrical power required	Combination code hard to secure, no indication / trace ability of who opened device
Electronic Combination - Key Pad	No key to lose, programmable	Combination code hard to secure, no indication / trace ability to who opened lock, electrical power required
Electronic Credential	Credential can be revoked without recovering device, inexpensive, established infrastructure	Counterfeit cards, lost cards, mechanical wear, electro / magnetic erasing
Barcode	Inexpensive to produce, under $1 a card	Easily counterfeited, subject to wear, ID has very limited data capacity, limited read range, light interference problems with some readers
Magnetic Stripe	Commonly used, mature technology, familiar user operation, inexpensive $1-3 card	Limited data capacity, subject to erasing and mechanical damage
Wiegand	Hard to duplicate, robust, non erasable	Long lead time for additional card, being replaced by Proximity, $5 each
Proximity	Non contact, low wear	More expensive than contact type cards, $4 and up
Smart Card	High security, data in card not system, large data capacity, used for Department of Defense Common Access Card (CAC), wide spread use in Europe for financial transaction	Mechanical wear, expensive $8+ cards, limited but growing market penetration
Proximity Smart Card	Non contract, low wear, less data storage than contact smart card, proposed for Transportation Worker Identification Credential (TWIC), next version of CAC	Expensive $10+ card, limited but growing market penetration, read range very limited (about 5 cm)
Other Cards	Hard to duplicate because of limited market	Limited market penetration and use
Biometric Credential	With proper tuning very high false reject rate and very high false acceptance rate, excellent method of identification and verification	Requires large data storage, more intrusive measurement method, higher computation processing power, problems with revocation of identifier
Finger Print - Optical	Inexpensive ($200), easy to use, small file size (250 Bytes)	Subject to counterfeit attack, problems with dirty fingers
Finger Print - Capacitive	Inexpensive ($300), easy to use, small file size (250 Bytes)	Moderate price, subject to counterfeit attack, problems with dirty fingers
Finger Print - Ultrasonic	Works with dirty fingers, harder to spoof with counterfeit, small file size (250 Bytes), high accuracy	Expensive ($2K), newer technology
Iris Scan	Easy to measure, moderate file size (512 Bytes), high accuracy, Inexpensive ($300 and up)	Works in biohazard suit, moderately easy to fool
Retinal Scan	Mature and fully developed, small biometric identification file, works on identical twins, small file size (96 Bytes) excellent false acceptance and rejection rates	Single product vendor, expensive system ($3K), large readers, slower response
Hand Geometry	Mature and fully developed, very small file size (9 Bytes)	Moderate Expense ($1.4K) and large readers, limited vendors
Face Scan	Fits into Photo as identification model, photos of user already on file, can use inexpensive camera and system ($1K)	Poor field operations and results, only works well under controlled imaging situations, facial changes degrades performance, face angle important, higher false rejection and acceptance rate, large file size (1.3 KB)
Voice Print	Easy to use	Not generally used for ACS, problems with noisy environments, pass code is audible to others, very large file size (2 to 10KB)
Signature	Familiar user operation	Signature hard to produce on input devices, used for business transaction not Access Control, large file size (1.5 KB)
Other Methods	-	In research and not commercially available

Table 25 - Access Control Systems – Access Control Devices, Data and Power Transmission, "Systems"

Access Control Systems	System Description	System Utilization
Access Control Devices		
Mechanical Lock	Door locks, pad locks, cabinet locks, etc.	Locking
Electric Strike Lock	Electromagnet control latch or strike	Addition of electronic control to existing lock system
Magnetic Lock	DC current energizes electro-magnet	Addition of locking device
Data and Power Transmission		
System Power	Power supply for door strikes, magnetic locks, access control panels, card readers, etc.	Use to access control system components
DC	DC powered system	Used for control panels, access control devices and magnetic locks
AC	AC line power system	Used for large loads such as electric strikes and computers systems
Control Signals	Methods to send control signal and control data	Credential read data, door control, computer control, ACS data
Wire	Metallic cable with insulation	-
Fiber Optic	Glass Fiber Optic cable with protective outer jacket	-
RF	Radio Frequency Wave	-
Systems		
Electronic Stand Alone	Single Stand Alone Reader and control system	Authenticates credential and opens control device (door, cabinet, etc.), monitors door status
Electronic Network	Multiple reader and control system	Network of card readers and access control systems
Integrated Systems	Integration of ACS with Intrusion Detection Sensors and Identification System	Provide a unified system for ACS, IDS, ID & Video Control

Table 26 - Access Control System - Access Control Devices, Data and Power Transmission, "Systems" Strengths and Weakness

Access Control Systems	System Strengths	System Weaknesses
Access Control Devices		
Mechanical Lock	Very mature technology, no electrical power required, common system with large support infrastructure, various level of security and robustness, competitive pricing	Lost key requires re-keying or replacement, no reco
Electric Strike Lock	Can be interfaced to fire / life safety system, can be overridden with key, mature technology with support infrastructure, record of use, available in fail safe or fail secure	Requires power, maintenance, and can stick, can b
Magnetic Lock	Can be interfaced to fire / life safety system, allow locking of glass, sliding, and other door not normally securable, very strong versions (over 600 lbs) available, can't be bypassed by key, fail safe, no maintenance required	Required power for operation, fail secure not availa
Data and Power Transmission		
System Power	Necessary	Must provide reliable and stable power for electroni loss of security, battery back up or similar system r
DC	Stable and quality power easily provided, simple battery back up	Voltage drops problems for long distance from supp suitable for larger system loads such as electric stri
AC	Large power loads easily accommodated	Stability and quality problems, reliable and clean po systems, loss of AC may mean loss of security
Control Signals	Required for operation	Control wiring must be secured from RFI, EMI, and
Wire	Inexpensive, easy to connect and install	Limited to shorter distances, subject to electro mag
Fiber Optic	Immune to EMI, allows long distance connections, interface from wire control to extend control distance	Expensive, requires special tools for installation an electric to optical conversion equipment
RF	No wire or fiber required	Expensive, subject to EMI, not secure, in higher fre line of sight only
"Systems"		
Electronic Stand Alone	Inexpensive, ideal for board or computer room door, mature technology, many systems and vendors available, usable single unit systems, some have plug in for computer used for configuration and back up	Not integrated into larger system, not easily upgrad back up
Electronic Network	Creates a systems of readers and access control equipment, mature technology with many systems and vendors available	Requires network wiring, clean and back up power, and power requirements, system configuration mor
Integrated Systems	Provide a method to fully integrate security functions of ACS, IDS, ID, and Video & Control	Complex and expensive systems, single vendors s source, requires clean and back up power, complex training and support expensive and complex, difficu sensors such as radar and sonar.

3.5.3 Costs

Access control system characteristics are only part of the information required to choose and appropriate systems. In addition implementation, maintenance, training, and life expectancy must be included in the selection criteria.

Tables 27 and 28 provide a summary of costs. Please note that even though materials costs and similar throughout the US, labor costs vary as much as 3 times and this will affect the amounts shown in the tables. Each authority will need to include this factor in implementation and support of the deployed systems.

The following tables provide a reference to estimated systems costs.

- Access Systems – A list of the types of lighting system
- Cost of Implementation – Rough range of installing system
- Cost of Maintenance – including operational costs expressed as a yearly % of implementation
- Cost of Training – extra or special training expressed as a one time % of implementation
- Life Expectancy – System life expectancy in years

Table 27 - Access Control Systems - Credentials and Biometric Credential Cost

System	Rough Cost of Implementation	Comments	Cost of Maintenance & Operation % per year	Comments	Cost of Training % one time	Comments	Life Expectancy
Credentials							
Mechanical Key	$1 to $10	Depends on design, patent, and security level	20%+	No maintenance, but considerable effort to maintain and track keys	20%	Lock smith and key production training, sometimes cost effective to send work out	20+ years
Mechanical Combination	$100 to $600	Depends on design and security level	20%+	Limited maintenance but update lock combination and service high use units	10%	Simple update and maintenance	10+ years
Electronic Combination - Key Pad	$250 to $1K	Simple install in place of adjacent to lock	<5%	Very low maintenance, need to replace battery on some units	<5%	Simple interface & control	10+ years
Electronic Credential Readers	-	-	-	-	-	-	-
Barcode	$100 to $500	Depends on range, resolution, indoor versus outdoor, stand alone versus PC required	5%	Cleaning of swipe type	5%	Requires training in theory of operation and trouble shooting	5 to 10 years
Magnetic Stripe	$100 to $500	Depends on style and read head durability	10%	Periodic head cleaning required, replacement of read head after swipe life exceeded	5%	Requires training in theory of operation and trouble shooting	5 to 7 years
Wiegand	$200 to $400	Depends on style and indoor versus outdoor	5%	Minimal maintenance, cleaning	5%	Requires training in theory of operation and trouble shooting	5 to 10 years
Proximity	$150 to $1K	Depends on range and style of reader	<5%	No regular maintenance required	5%	Requires training in theory of operation and trouble shooting	10+ years
Smart Card	$40 to $500	Depends on stand alone or PC required and quantity	5%	Contact cleaning	10%	Requires training in theory of operation and trouble shooting	5 to 7 years
Proximity Smart Card	$2K to $4K	Depends on range, style & quantity	<5%	No regular maintenance required	10%	Requires training in theory of operation and trouble shooting	10+ years
Biometric Credential							
Finger Print - Optical	$150 to $1K	Require PC for control	10%	Cleaning and PC support	10%	Methods of registration, maintenance of data base	5 to 7 years
Finger Print - Capacitive	$350 to $2K	Require PC for control	10%	Cleaning and PC support	10%	Methods of registration, maintenance of data base	5 to 7 years
Finger Print - Ultrasonic	$2K to $3K	Stand Alone with network connection	5%	Cleaning	10%	Methods of registration, maintenance of data base	5 to 7 years
Iris Scan	$200 to $2K	Require PC for control	15%	Cleaning and PC support	10%	Methods of registration, maintenance of data base	5 to 7 years
Retinal Scan	$3K to $5K	Stand Alone with network connection	5%	Cleaning	10%	Methods of registration, maintenance of data base	5 to 7 years
Hand Geometry	$3K to $5K	Stand Alone with network connection	5%	Cleaning	10%	Methods of registration, maintenance of data base	5 to 7 years
Face Scan	$2K to $5K	Require PC for image processing and control	15%	Support of computer	15%	Methods of registration, maintenance of data base, support of computer system	5 to 7 years

Table 28 - Access Control Systems – Access Control Devices, Data and Power Transmission, Systems Costs

System	Rough Cost of Implementation	Comments	Cost of Maintenance & Operation % per year	Comments	Cost of Training % one time	Comments	Life Expectancy
Access Control Devices							
Mechanical Lock	$50 to $150	Depends on design and security level	25%	Requires minimal adjustment and repair. Expense in maintenance of key inventory	5%	Standard locks and keys	20+ years
Electric Strike Lock	$150 to $500	Depends on design and security level	20%	Requires adjustment of strike and door, lubrication of strike	5%	Mechanics simple and straight forward	5 to 15 years depending on use and abuse
Magnetic Lock	$350 to $700	Depends on design and security level	<5%	Very low maintenance	<5%	Simple training on theory and operation	10+ years
Data and Power Transmission							
System Power	-	-	-	-	-	-	-
DC	$100 to $350	Small AC to DC power supply with battery	5%	Battery replacement every 3 to 5 years	0%	None	10+ years
AC	$20+	AC transformer	<5%	No maintenance	0%	None	10+ years
Control Signals	-	-	-	-	-	-	-
Wire	$.50 to $3 foot	Wires for readers, power supplies, and network (access control and data)	<5%	Little to no maintenance	<5%	Training on camera control	10+ years
Fiber Optic	Cable $1+ per foot, Converters $500 to $2K each	Require electro-optic converters, highly dependant on distance	<5%	Little to no maintenance	25%	Training on fiber optics methods, testing, maintenance, and safety	10+ years
RF	$2K to $50K	Radio link dependant of frequency, distance, and line of sight	10%	Routing antenna alignment, cleaning and frequency check	20%	RF and control set up and maintenance	5 to 10 years
Systems							
Electronic Stand Alone	$2K to $5K	Some require PC for programming	20%	Maintain system and update of configuration of changing users	20%	Configuration, update, and routine maintenance	5 to 7 years
Electronic Network	$5K to $500K	System to connect multiple readers, very dependant on size and topology of network	20%	Cost greatly dependant of network upkeep and maintenance, can be much lower	10%	Standard computer type of network	10+ years
Integrated Systems	$25 to $4M	Depends on size, number of readers, remote location, number of users, etc.	20%	Support includes large computer system, network, power supplies, card readers, data base, and configuration	5% to 10%	Training on system maintenance, configuration, and support	5 to 10 years

3.5.4 Other Factors

There are other factors that must also be considered in the implementation of ACS. These include, but are not limited to the following.

- Privacy concerns of historical access records
- Work rule concerns of access records
- Legal implications of access control operation or failure to operate
- A system for archiving of access records must be established and supported. This includes, but is not limited to the following
  - Legal requirement
  - Chain of custody
  - Storage medium selection
  - Secure and temperature controlled storage area
  - A method to retrieve and return archived information

3.6 SENSOR SYSTEMS

3.6.1 Technology

The heart of Intrusion Detection Systems (IDS) is the various sensor systems used to detect violation into a protected area. Information for system design is used to choose and locate sensors. This section describes the types of available sensors, their application, and relative cost.

To provide background information, the below data is provided in the following tables.

- Annunciation Input – a description of IDS alarm annunciation and alarm classes
- Sensor Processing – description of function
- Data Fusion & Display – definitions
- Sensor Types – generic classification of sensors and their application

The authors intentionally omitted a "Cost" data sheet related to Table 29 and Table 30 due to the fact that these two tables are used primarily to discuss general and wide-ranging technology topics. These Sensor System features (Annunciation Input, Sensor Processing, Data Fusion & Display, and Sensor Types) should be considered as overall "general" topics. When focusing more directly on specific types of sensor technologies (Table 31 through Table 36), cost data sheets for these sensor systems are provided as Tables 38, 39, and 40.

Table 29 - Sensor Systems – Annunciation Input, Data Fusion & Display, Sensor Types

Sensor Systems	System Description	System Utilization
Annunciation Input		
Description	Digital input to annunciate alarm condition, result of alarm trip or output of alarm processing system. Result is contact closure or contact open	Method to annunciate alarm condition
Grade B	Digital input annunciation with normally open or normally closed contact, state change annunciates alarm	Alarm annunciation
Grade A	Supervise alarm input with line and sensor resistor	Alarm annunciation
Grade AA	Response / Interrogation for alarm sensor	Alarm annunciation
Sensor Processing	Equipment and computer processors that receive sensor inputs and determine if an alarm condition exists. Provide binary output of processing decision	Use to determine if sensor excitation is actual alarm, not required for binary sensor devices
Data Fusion & Display		
Remote Data Integration Sensors	System to collect at field site, inputs from various sensor systems	Lessen cabling and communication requirements for large number of sensors
Alarm Reporting Map Display Systems	Computer or mimic mapping system to display sensor layout zones and to annunciated conditions and alarms	A method to provide human monitoring for alarms and system status
Sensor Types		
Interior	Sensor installed inside building and structure interiors	Sensors for interior use and moderate environmental conditions
Exterior	Sensor installed in outdoor locations, also used in harsh indoor environments	Exterior and Harsh environments, can be used for interior sensors
Area Sensor	Sensor used to monitor a physical surface area such as a floor, outdoor ground area, etc. Can be simple as pressure mat to buried field sensor. Distinction between Area and Volume sensors are sometimes limited	Used to monitor 2-dimensional surfaces that intruder crosses during system penetration
Barrier Sensors	Sensors used to monitor a physical barrier - fence, wall, roof, window, etc.	Sensor annunciates physical modification or attack of barrier
Point Sensors	A sensor that is used to monitor a single point such as door position (open or closed)	Used for barrier that "close": doors, windows, cabinets, safe doors, etc
Volume Sensors	Sensor used to monitor a physical space such as room interior, volume around a door, or volume adjacent to a fence	Used to monitor 3-dimensional volumes that intruder enter during system penetration

Table 30 - Sensor Systems - Annunciation Input, Data Fusion & Display, Sensor Types Strengths and Weaknesses

Sensor Systems	System Strengths	System Weaknesses
Annunciation Input		
Description	Simple Yes / No binary output	**Alarm Processing** - evaluation of input data to determine whether to announce alarm condition **Intrusion Alarm** - annunciation of alarm resulting from detection of specified target attempting to intrude into protected area **Nuisance Alarm** - annunciation of alarm by detection of stimuli that is not attempt to intrude into protected area **Environmental Alarm** - annunciation of alarm resulting from environmental conditions **False Alarm** - annunciation of alarm with no alarm stimuli
Grade B	Simple equipment & design	Easily subject to bypass, system failures not annunciated to system
Grade A	Annunciates system and equipment failure, straight forward installation	Can be defeated by meticulous expert
Grade AA	Extremely high security	Extremely difficult to bypass, complex and more expensive, circuit after AA device is grade A or B
Sensor Processing	Provides method to determine Intrusion vs. Nuisance vs. Environmental Alarm, System can be tuned and trained to sensor characteristics installation environmental conditions	Expensive, conflicting requirements for alarms conditions, improper setting lowers probability of detection, must be tuned and trained to sensor and environmental conditions of installation
Data Fusion & Display		
Remote Data Integration Sensors	Less field wiring, low power consumption, easier to upgrade and add sensors	If integration device fails, system will lose all sensors connected to device
Alarm Reporting Map Display Systems	Superior human interface, allows both alarm and condition monitoring of sensors, industry standard	More expensive and complex than simple on / off notification (Example - red light)
Sensor Types		
Interior	Less expenses, more sensitive, than exterior devices	Less physically and environmentally robust
Exterior	Physically and environmentally robust	More expensive and less sensitive than interior sensors
Area Sensor	Normally hidden from intruder view, provide excellent back up to other sensors	Sensor zone can be bridged or jumped over, requires sensor processing for advanced systems
Barrier Sensors	Provide annunciation of physical attack	Barrier is normally damaged or altered to initiate sensor alarm, sensor processing required
Point Sensors	Simple, easy to install, readily available, binary output (no signal processing required)	Point can be bypass physically (cut hole in door instead of open door), sensor can be bypassed
Volume Sensors	Excellent method to define and monitor secure volume, excellent results for interior volumes	Sensor can sometimes be masked, require sensor processing, can be subject to nuisance alarms, sometime difficult to properly design and adjust for outdoor uses

3.6.2 Applications

Sensor systems technologies cover the spectrum from simple push button switches to complex radar. The following tables provide a summary of the systems. Note that in addition to sensing intrusion, IDS can also provide historical data that can assist post incident analysis. The columns are as follows :

- Sensor Systems – A list of the types of systems and equipment available
- System Description – A short description of the systems and equipment
- System Utilization – The application of the system
- Systems Strengths – Positive attributes of the system
- System Weaknesses – Negative attributes of the system

Table 31 - Sensor Systems – Binary Sensors, Buried Sensors, Fence Sensors

Sensor Systems	System Description	System Utilization
Binary Sensors	Intrusion annunciation by change of contact state - open to closed or closed to open, no signal processing	Point and Area sensor for interior and exterior use
Balance Magnetic Switch	Binary device used to indicate closed or open status, balance magnetic used to prevent external bypass via magnet	Point sensor for interior or exterior use
Breakwire	Intrusion into protected area cause break of wire and annunciation alarm	Point sensor for interior use
Call Box Alarm	Push button activated alarm (special application of duress alarm)	Use in Transit Agencies
Duress Alarm	Push button activated by finger, foot, or removable on money. Wire or wireless	Point sensor for interior or exterior use
Electric eye / Photo Electric Eye	Optical beam of light projected from source to sensor, low end annunciation use	Area interior sensor
Foil	Thin foil attached to windows, broken glass breaks (open circuits) foil	Barrier Penetration Sensor for Interior use
Magnetic Switch	Magnet hold alarm switch in one state, intrusion cause change of state	Point interior sensor
Mechanical Switch	Mechanical switch that changes state when point is changed by intruder	Point Sensor
Pressure Sensor / Mats / Switch	Mat or carpet or similar device wired with switch, when intruder steps on sensor, switch changes state to annunciate alarm	Area sensor for interior use
Security Screen	Wire mesh loop placed in Insect screen, wall or other barrier device, cut or removal of device annunciated alarm	Barrier Penetration Sensor for Interior or Exterior use
Buried Sensors	Sensors buried in ground on secure side of barrier, typically fence - consist of a class of detection methods	Area Exterior Sensor
Balanced Pressure Buried	Tubing / Pipe buried installed under floor and filled with fluid, pressure on tube cause alarm, balancing circuit used to compensate for changing environment conditions	Area Sensor for both internal and external use
Fiber Optic Cable	Fiber cable buried under surface senses intruder by variations in light transmission	Area Sensor for both internal and external use
Geophone Buried	Buried sensor that listens for shock and vibration of intrusion. Adaptation from seismologists / geophysicist instrumentation	Area Exterior Sensor
Ported Coaxial Buried Line	Coaxial cable with "port" or openings in shield conductor that allow leakage of RF signal injected into cable. Alteration of leaked field by intruder activates alarm	Area Exterior Sensor
Fence Sensors	Sensors attached to fence and other barriers to monitor disturbance and attacks	Barrier Sensor normally for external use
Capacitive Cable	Changes in capacitance of cable caused by intrusion annunciates alarm	Barrier Sensor normally for external use
Electric Field / Electrostatic Field	Minimum of 3 wires installed on insulated stand off. One (or more) signal wires and two (or more) sense wires. Interruption of electric field by intruder annunciates alarm.	Barrier Sensor normally for external use
Fiber Optic Cable / Mesh	Fiber optic cable or mesh installed on fence. Disturbance of fence modulates light or in the case of a cut stops light	Barrier Sensor for Exterior and Interior use
Geophone / Microphone Fence	Sensor that measures shock and vibration of monitored fence	Barrier Sensor normally for external use
Taut Wire / Tension Sensor	Wire is installed tightly to fence structure, sensor processor monitors fence movement and tamper, alarms when criteria is met	Barrier Sensor normally for external use

Table 32 - Sensor Systems – Fixed Barrier/Wall Sensors, Infrared Sensors, Microwave Sensors

Sensor Systems	System Description	System Utilization
Fixed Barrier / Wall Sensors	Sensors embedded into wall or barrier to monitor disturbance and attacks	Barrier Sensor for internal and external use
Capacitive Cable	Changes in capacitance of cable caused by intrusion annunciates alarm	Barrier Sensor for Exterior and Interior use
Fiber Optic Cable / Mesh	Fiber optic cable or mesh installed in wall or barrier. Disturbance of wall modulates light or in the case of a break stops light	Barrier Sensor for Exterior and Interior use
Geophone Wall	Sensor that measures shock and vibration of monitored wall	Barrier Sensor for Exterior and Interior use
Infrared Sensors	Sensor that utilized Infrared (IR) light (between .7 to 15 microns) to detect intrusion. Source can be Light Emitting Diode (LED) or laser. Systems also include passive sensors that detect presence of IR light from intruder	Volume and Area Sensors for interior and exterior use
Infrared Beambreak Detector	Pair of IR devices consisting of IR transmitter and IR receiver. Transmitter forms beam of microwave energy that when disturbed by intruder is detected at IR receiver. Senses motion and blockage. Systems use multiple beams to reduce nuisance alarms.	Area Sensors for interior and exterior use
Passive Infrared Sensor / Detector (Heat sensor)	IR light detector sensor calibrated to sense heat output from intruder, filters used to eliminate other source of IR	Volume Sensor for interior and exterior use
Laser Scanning System	Short Tower system with laser scanner that maps a contour of a 360 degree area around sensor, intruder into area changes contain and annunciates alarm	Volume Sensor for exterior use
Microwave Sensors	Sensor system that emits and receives microwave energy, modulation or interruption of energy annunciates alarm	Volume Sensor for Exterior or Interior use
Microwave Bistatic	Pair of microwave devices consisting of microwave transmitter and microwave receiver. Transmitter forms cone of microwave energy that when disturbed by intruder is detected at microwave receiver. Senses motion and blockage.	Volume sensor for exterior use
Microwave Monostatic	Single sensor with transmitter and receiver housed in same physical unit, disturbance of microwave energy annunciates alarm	Volume Sensor for Exterior or Interior use
Radar	Land, air, and water surface detection of people, vehicles, boats and other objects	Volume and Area sensor for external use
Radar Vehicle Detectors	Self contained radar unit designed to detect and count vehicles	Volume and Area sensor for external use

Table 33 - Sensor Systems- Binary Sensors, Buried Sensors, Fence Sensors Strengths and Weaknesses

Sensor Systems	System Strengths	System Weaknesses
Binary Sensors	Simple, no processing required	Subject to high nuisance alarm rate
Balance Magnetic Switch	Binary open or closed, difficult to bypass with external magnet	Bypass of barrier that sensor is attached to
Breakwire	Simple binary input and installation	Wire tension must be maintained, alarm requires replacement of wire, not commonly used
Duress Alarm	Binary open or closed	Must be covertly installed and activated to prevent harm to personnel activating alarm
Electric eye / Photo Electric Eye	Binary response, inexpensive	Easily bypassed and observed, visible light systems not commonly used in commercial / industrial security, high nuisance alarm rate, replaced by IR Beam sensors
Foil	None	Not used in new installation, Maintenance problem, foil easy broken by thermal shifts of glass and glass cleaning, difficult to repair, can be bypassed, glass break detectors now used
Magnetic Switch	Very inexpensive	Easy bypass with external magnet, replace by balance magnetic switches
Mechanical Switch	Micro-switches in limited use for door open sensors	Not commonly used, maintenance and contact problems
Pressure Sensor / Mats / Switch	Simple binary input and installation, used for backup	Maintenance problems, easy to bypass or jump over, easily to identify
Security Screen	Simple, easy to install, allow secure open window	Subject to damage and misalignment of screen, must added magnetic switch to preclude removal of screen, relatively easy to bypass
Buried Sensors	Can follow contour of ground line, hidden from view	Some systems require areas preparation versus simple trenching. Proper back fill and tamping required to prevent cable damage. Requires processing equipment and different calibration for different materials - dirt, concrete, grass, etc. Detect above as well as below ground so underground utilities may present operational problems and nuisance alarms, buried cables subject to rodent and erosion damage
Balanced Pressure Buried	Electromagnetic and Radio Frequency immune	High maintenance, no longer supported, fluid leakage, imbalance leads to false alarms, now replaced by other area sensors - fiber optic, ported cables, etc.
Fiber Optic Cable	Immune to EMI / RFI interference, proper installation and calibration provide a reliable low nuisance alarm results	Requires signal processing, area must be prepared with excavation and proper fill, snow may prevent detection of intruder, difficult to service and replace, subject to rodent and erosion damage
Geophone Buried	Hidden from view, low maintenance for factory sealed and properly installed system	Requires signal processing, area must be prepared with excavation and proper fill, snow may prevent detection of intruder, difficult to service and replace, subject to rodent and erosion damage
Ported Coaxial Buried Line	Simple trench installation, several vendors, established technology	Field can be detected with proper instrumentation
Fence Sensors	Can retrofit existing fence, installation straight forward	Visible, requires fence to be maintained in good repair, subject to vandalism, most systems require sensor processor
Capacitive Cable	Can retrofit existing fence, installation straight forward	Cable age and degradation cases nuisance problems, requires recalibration, sensor processing required, low use
Electric Field / Electrostatic Field	Can retrofit existing fence, installation straight forward, normally easy to trouble shoot and repair	Very visible, subject to damage, proper wire tensioning must be maintained, subject to EMI / RFI interference
Fiber Optic Cable / Mesh	Can retrofit existing fence, installation straight forward, immune to EMI / RFI interference, proper installation and calibration provide a reliable low nuisance alarm result	Fiber cable installation, maintenance, and repair requires special tools and test equipment
Geophone / Microphone Fence	Good immunity to nuisance alarms, easy retrofit installation, very low maintenance for factory delivered sealed units	Require sensor processing system, visible on fence
Taut Wire / Tension Sensor	Can retrofit existing fence, installation straight forward, normally easy to trouble shoot and repair	Require sensor processing system, visible on fence, proper tension must be maintained

Table 34 - Sensor Systems - Fixed Barrier/Wall Sensors, Infrared Sensors, Microwave Sensors Strengths and Weaknesses

Sensor Systems	System Strengths	System Weaknesses
Fixed Barrier / Wall Sensors	Invisible	Must be installed during construction, difficult or impossible to repair or replace
Capacitive Cable	None	Cable age and degradation cases nuisance problems, requires recalibration, sensor processing required, low use
Fiber Optic Cable / Mesh	Immune to EMI / RFI interference, proper installation and calibration provide a reliable low nuisance alarm results	Fiber cable installation, maintenance, and repair requires special tools and test equipment, require sensor processing
Geophone Wall	Good immunity to nuisance alarms, very low maintenance for factory delivered sealed units, can be added to existing structures	Requires sensor processing system
Infrared Sensors	Invisible to the un-aided eye, numerous vendors and supplies, large range of sensors for short, long, exterior, and interior applications, can operate with simple sensor processing, passive sensor difficult to detect	Visible with proper instrumentation
Infrared Beambreak Detector	Provide effective "wall" or IR light to detect intrusion into protected zone. Provides coverage for precisely defined area, established technology with numerous vendors, and systems.	IR light "visible" with proper equipment, multi beam system required to prevent nuisance alarms
Passive Infrared Sensor / Detector (Heat sensor)	Passive mode, effective coverage of covered zone, single self contained unit, established technology with numerous vendors, and systems.	Need clear zone, limited range cutout contributes to nuisance alarms, will not detect insulated intruder
Laser Scanning System	Very effective coverage of intrusion zone.	Expensive, system is visible and subject to vandalism, contour may present some dead zones
Microwave Sensors	Invisible, Large selection of types and applications, mature technology	Requires signal process and complex setup, installation area must be properly prepared to achieve low nuisance alarm rate, standing water causes alarm problems
Microwave Bistatic	Effective coverage of large clear areas, can provide high security coverage, sensor processor can be tuned for low nuisance alarms rates	Line of sight only, terrain variations cause dead zones, require proper installation and alignment, vegetation must be kept short and standing water prevented
Microwave Monostatic	Effective coverage or limited areas, range gate prevents out of zone nuisance alarms, numerous vendors, suppliers, and systems for interior use	Line of sight only, terrain variation causes dead zone, require proper installation and alignment, vegetation must be kept short and standing water prevented
Radar	Long range detection and tracking of surface and air targets, works in low to zero visibility conditions	Expensive, requires complex control, tuning, setup, and display
Radar Vehicle Detectors	Special application of monostatic sensor for vehicle detections	Works with vehicle and other large objects only

Table 35 - Sensor Systems – Other Sensors and Sound Sensors

Sensor Systems	System Description	System Utilization
Other Sensors		
Capacitance	Sensor uses capacitance change to measure intrusion into protected zone, change in distance of capacitive plate cause large change in capacitance	Point sensor for interior use
Dual Technology Passive IR/Microwave	Combines IR and Microwave technologies into one sensor	Volume for interior and exterior use
Magnetic Anomaly Detection (MAD)	Sensor used to detect anomaly or changes in the earth's magnetic field	Area Exterior Sensor
Metal Detectors	Uses either induced balance, pulse induced or beat frequency oscillation to detect metal, Mostly for personnel scanning for presence of metal	Area Interior and Exterior sensor
Piezoelectric	Solid state crystal that emits a voltage signal when compressed, also used in microphones	Area Interior Sensors
Strain Sensitive Cable	Fence Sensors, mechanical vibration	Barrier for exterior and interior sensors
Sound Sensors		
Acoustic / Audio / Sound Sensor (Microphone)	Microphonic device that listens for sounds of intrusion (tools, breathing, heartbeat, etc.), can use infrasonic (less than 20 Hz), audible (20 Hz to 20 KHz) or ultrasonic (above 20 KHz) sounds	Intruder causes noise in protected zone
Acoustic Detection (Air Turbulence)	Acoustic sensor that measures air motion	Intruder causes air motion, Volumetric / Interior use only
Glass Break Sensors	Volume	Interior Sensors - Signal Processors
Sonar	Injection of acoustic energy into water volume to detect intrusion of divers & submersibles	Volume sensor for underwater use
Ultrasonic Motion Detector	Sensor emits ultrasonic sound and detects Doppler shifts caused by intruder	Volume sensor for interior use
Vibration Sensor	High frequency vibrations from oxyacetylene torches, oxygen lance, drills, saws, explosives	Barrier Sensor for Interior use
Video Motion Sensors	Uses video signal input and image processing to detect intrusion into secure area. Methods include pixel comparison, temporal comparison, light threshold, etc.	Volume Sensor for Exterior or Interior use
Alarm Confirmation	Upon tripping of intrusion sensor, video system is directed toward alarm area to confirm and investigate alarm	Volume Sensor for Exterior or Interior use
Analog Systems	Uses analog signal processing techniques to determine alarm conditions and alarm annunciation	-
Digital Systems	Uses digital signal processing techniques to determine alarm conditions and alarm annunciation	-

Table 36 - Sensor Systems – Other Sensors and Sound Sensors Strengths and Weaknesses

Sensor Systems	System Strengths	System Weaknesses
Other Sensors		
Capacitance	No moving parts, can be very sensitive to intrusion	Requires signal processing, equipment must be electrically isolated
Dual Technology Passive IR/Microwave	Combine two technologies to ensure intrusion detection and low nuisance alarm rate	Limited
Magnetic Anomaly Detection (MAD)	Can be buried, installed in door ways	Will not detect intruder with no metal or magnetic disturbing equipment, require sensor processor, used for military applications
Metal Detectors	Numerous vendors and supplies, mature technology	Will not detect intruder with no metal or magnetic disturbing equipment
Piezoelectric	Robust, limited signal processing required	Requires signal processing, normally installed during construction, difficult to replace / repair
Strain Sensitive Cable	Easily installed	Requires signal processing, cable characteristic changes cause calibration problems
Sound Sensors		
Acoustic / Audio / Sound Sensor (Microphone)	Used as secondary back up to other technologies, can be used to listen in on protected zone	High nuisance alarm rates for non intrusion sounds, can require sophisticated sensor processing
Acoustic Detection (Air Turbulence)	Limited	Limited vendor support, non standard, limited interior use only, replaceable by numerous other sensor types - Microwave, IR, etc.
Glass Break Sensors	Easy to install, one device can monitor multiple windows, inexpensive test devices available	Requires signal processing, can be bypassed by cutting glass
Sonar	Provides detection of underwater approaches to valuable structures and systems	Expensive, requires advanced sensor processing, output display normally on stand alone display unit
Ultrasonic Motion Detector	Limited	Subject to dead zones, obsolete for intrusion detection
Vibration Sensor	Effective in monitoring certain intrusion attempt sounds and vibrations	Special application with limited use, requires sensor processing
Video Motion Sensors	Leverages existing video system to added intrusion detection and alarm	Requires proper set up and calibration, subject to nuisance alarms
Alarm Confirmation	Allows easy confirmation of sensor alarms, can be used to tune and adjust sensor processor settings	Requires integration of intrusion sensors alarm system with video and video control system
Analog Systems	Inexpensive, used for very small system	Hard to calibrate and adjust, subject to high nuisance alarm rate, falling into disuse
Digital Systems	Very capable with selected exclusion zones and alarm criteria, wide selection of vendors and technologies, software upgrades possible on existing equipment, systems available to support large camera installations	Can be expensive and difficult to set up, confusing array of systems and technologies, still subject to nuisance alarms

3.6.3 Costs

Sensor characteristics are only part of the information required to choose an appropriate system. In addition implementation, maintenance, training, and life expectancy must be included in the selection criteria.

Table 37 indicates a relative cost comparison of a sampling of various classes of sensors with L = low, M = medium, and H = high designated as the relative cost factors.

Table 37 - Sensor System Relative Cost Comparison

Type of Sensor	Equipment	Installation	Maintenance
Fence Mounted	L	L	L
Taut Wire	H	H	M
Electric Field	H	M	M
Capacitance	M	L	M
Ported Cable	H	M	M
Seismic / Acoustic	M	M	L
Magnetic	H	M	L
Microwave	M	L	H
IR	M	L	M
Video Motion	M	L	M

A more complete cost comparison is included in Table 38. Please note that even though materials costs are similar throughout the US, labor costs vary as much as 3 times and this will affect the amounts shown in the tables. Each authority will need to include this factor in implementation and support of the deployed systems.

- Sensor Systems – a list of the types of sensors system
- Cost of Implementation – rough range of installing system
- Cost of Maintenance – including operational costs expressed as a yearly % of implementation
- Cost of Training – extra or special training expressed as a one time % of implementation
- Life Expectancy – system life expectancy in years

Table 38 - Sensor Systems Cost – Binary Sensors, Buried Sensors, Fence Sensor Systems

System	Rough Cost of Implementation	Comments	Cost of Maintenance & Operation % per year	Comments	Cost of Training % one time	Comments	Life Expectancy
Binary Sensors							
Balance Magnetic Switch	$50 to $250	Depends on range, cable style and housing	<5%	Very Low Maintenance	<5%	Minimal Training	20+ years
Breakwire	$50 to $150	Mostly obsolete because wire must be replaced after activation	25+%	Activation requires breakwire to be replaced. Wire tension must be adjusted	<5%	Minimal Training	10+ with no operation
Duress Alarm	$5 to $150	Hardwire versus RF link, foot switch versus push button or micro-switch	<5%	Very Low Maintenance	<5%	Minimal Training	20+ years
Electric eye / Photo Electric Eye	-	See - Infrared Beambreak Detector - below	-	-	-	-	-
Foil	-	Obsolete - see glass break detectors in the next Table	-	-	-	-	-
Magnetic Switch	$5 to $20	Simple low device	<5%	Very Low Maintenance	<5%	Minimal Training	20+ years
Mechanical Switch	$5 to $21	Simple device with limited application	20%	Prone to contact failure	<5%	Minimal Training	10 years
Pressure Sensor / Mats / Switch	$50 to $150	Limited application	25+%	Subject to wear and contact failure, replacement instead of repair	<5%	Minimal Training	3+ years, depends on use
Security Screen	$50 to $150	Depends on size	20%	Subject to damage when screens are cleaned	<5%	Minimal Training	5+ years, depends on corrosive environment
Buried Sensors							
Balanced Pressure Buried	-	Obsolete	-	-	-	-	-
Fiber Optic Cable	$20K & up Cable $3 foot & up	Requires software, processor module, power supply and cable	10%	Minimal maintenance if cable not disturbed	10%	Requires training in theory of operation, calibration and set up	10+ years
Geophone Buried	$20K & up	Requires software, processor module, power supply and cable	20%	Geophones may need replacement	10%	Requires training in theory of operation, calibration and set up	10+ years
Ported Coax Buried Line	$20K & up Cable $3 foot & up	Requires software, processor module, power supply and cable	10%	Minimal maintenance if cable not disturbed	10%	Requires training in theory of operation, calibration and set up	10+ years
Fence Sensor Systems							
Capacitive Cable	$20K & up Cable $3 foot & up	Requires software, processor module, power supply and cable	10%	Minimal maintenance if cable not disturbed	10%	Requires training in theory of operation, calibration and set up	10+ years
Electric Field / Electrostatic Field	$20K & up Cable $3 foot & up	Requires software, processor module, power supply and cable	10%	Minimal maintenance if cable not disturbed	10%	Requires training in theory of operation, calibration and set up	10+ years
Fiber Optic Cable / Mesh	$60 to $100 a foot	Requires software, processor module, power supply and cable	<5%	Very Low Maintenance	5%	Requires training in theory of operation, calibration and set up	10 - 15+ years
Geophone / Microphone Fence	$20K & up	Requires software, processor module, power supply and cable	20%	Geophones may need replacement	10%	Requires training in theory of operation, calibration and set up	10+ years
Taut Wire / Tension Sensor	$5K & up	Requires software, processor module, power supply and cable	20%	High Maintenance, yearly adjustment required	5%	Requires training in theory of operation, calibration and set up	5 to 10+ years

Table 39 - Sensor Systems Cost - Fixed Barrier/Wall Sensors, Infrared Sensors, Microwave Sensors

System	Rough Cost of Implementation	Comments	Cost of Maintenance & Operation % per year	Comments	Cost of Training % one time	Comments	Life Expectancy
Fixed Barrier / Wall Sensors							
Capacitive Cable	-	Similar to fence systems	-	-	-	-	-
Fiber Optic Cable / Mesh	-	Similar to fence systems	-	-	-	-	-
Geophone Wall	-	Similar to fence systems	-	-	-	-	-
Infrared Sensors							
Infrared Beambreak Detector	$200 to $1K	Depends on range, pattern, beam pattern, indoor versus outdoor	<5%	Very Low Maintenance	5%	Requires training in theory of operation, calibration and set up	5 to 10+ years
Passive Infrared Sensor / Detector (Heat sensor)	$50 to $500	Depends on range, pattern, beam pattern, indoor versus outdoor	<5%	Very Low Maintenance	5%	Requires training in theory of operation, calibration and set up	5 to 10+ years
Laser Scanning System	$75K to $150K	Estimated Price $100K	5%	Recalibration, cleaning	10%	Requires training in theory of operation, calibration and set up	5 to 10+ years
Microwave Sensors							
Microwave Bistatic	$3K to $5K	System pair (transmitter & receiver)	<5%	Very Low Maintenance	5%	Requires training in theory of operation, calibration and set up	10+ years
Microwave Monostatic	$3K to $5K	Self contained unit	<5%	Very Low Maintenance	5%	Requires training in theory of operation, calibration and set up	10+ years
Radar	$50K to $250K+	Depends on range and software processing	10%	Recalibration of exclusion zones, preventive maintenance	10%	Requires training in theory of operation, calibration and set up	10+ years
Radar Vehicle Detectors	$15K to $30K	Self contained unit with RS-232 interface	<5%	Very Low Maintenance	5%	Requires training in theory of operation, calibration and set up	10+ years

Table 40 - Sensor System - Other Sensors, Sound Sensors, Video Motion Sensors Cost

System	Rough Cost of Implementation	Comments	Cost of Maintenance & Operation % per year	Comments	Cost of Training % one time	Comments	Life Expectancy
Other Sensors							
Capacitance	$300 to $1K	Depends on application & processor	10%	Minimal maintenance	5%	Requires training in theory of operation, calibration and set up	5 to 10 years
Dual Technology Passive IR/Microwave	$100 to $800	Depends on range, pattern, beam pattern, indoor versus outdoor	<5%	Very Low Maintenance	5%	Requires training in theory of operation, calibration and set up	5 to 10+ years
Magnetic Anomaly Detection (MAD)	$1K and up	Depends on number of zones, vehicles versus people	5%	Low Maintenance	5%	Requires training in theory of operation, calibration and set up	6 to 10+ years
Metal Detectors	$200 to $5K+	Depends on configuration, range and operation	10%	Minimal maintenance	5%	Requires training in theory of operation, calibration and set up	5 to 10+ years
Piezoelectric	$20K & up	System requires software, processor module, power supply and cable	10%	Minimal maintenance	10%	Requires training in theory of operation, calibration and set up	6 to 10+ years
Strain Sensitive Cable	$20K & up Cable $3 foot & up	System requires software, processor module, power supply and cable	10+%	Maintenance dependant of physical abuse. Recalibration required depending on system monitored	10%	Requires training in theory of operation, calibration and set up	5 to 10+ years
Sound Sensors							
Acoustic / Audio / Sound Sensor (Microphone)	$1K & up	Depends on processing methods and equipment	10%	Minimal maintenance	5%	Requires training in theory of operation, calibration and set up	10+ years
Acoustic Detection (Air Turbulence)	$1K & up	Depends on processing methods and equipment	10%	Minimal maintenance	5%	Requires training in theory of operation, calibration and set up	10+ years
Glass Break Sensors	$40 to $150	Built in sensor processing with alarm contact output	<5%	Very Low Maintenance	10%	Glass break simulator required to test	10+ years
Sonar	$500K to $1M	Requires custom design and installation, cost is for single system zone, added zones are less	5%	Requires cleaning of marine growth, protection from damage, & realignment	5%	Requires training in theory of operation, calibration and set up	10+ years
Ultrasonic Motion Detector	-	Obsolete - use IR or Dual Technology	-	-	-	-	-
Vibration Sensor	-	Similar to Acoustic Detector above	-	-	-	-	-
Video Motion Sensors							
Analog Systems	$300 to $600	Single channel	<5%	Very Low Maintenance	5%	Requires training in theory of operation, calibration and set up	10+ years
Digital Systems	$2K and up	Depends on number of channels, can be either stand alone unit or software running on PC	<5%	Very Low Maintenance	10%	Requires training in theory of operation, calibration and set up	10+ years

3.6.4 Other Factors

There are other factors that must also be considered in the implementation of Sensor Systems. These include, but are not limited to the following:

- Impact of alarm suppression and control on work flow
- Impact of "cry wolf" syndrome (ignoring alarms after multiple false alarms) for poorly functioning sensor systems
- Legal implications of sensor systems operation or failure to operate
- A system for archiving alarm data must be established and supported. This includes, but is not limited to the following:
  - Legal requirement
  - Chain of custody
  - Storage medium selection
  - Secure and temperature controlled storage area
  - A method to retrieve and return archived information

3.7 IDENTIFICATION SYSTEMS

3.7.1 Technology

In order to control personnel access into secured area a method of identification is required. Identification technologies are used to create a credential that can be used by both security personnel and electronic access control systems to uniquely identify authorization status. Security workers use graphics, colors, pictures, and text to help identify personnel. Typically this includes name, a color picture, graphics to identify the authority and additional identification, training, and safety data. For electronic access control, an identification method is embedded into a card to allow reading of unique data. For example, this data could include magnetic encoded information, user biometrics template, or RF identification numbers.

3.7.2 Applications

The controlling authority designs the layout and look of the badge, while the ACS data is determined by the technology selected for the access control system. Identification systems provide a method to register personnel, record personal data, encode ACS information and issue a credential – typically called a 'badge' or 'access card'.

Tables 41 and 42 provide a reference to available technologies and systems. Columns are as follows:

- Identification System – A list of the generic types systems
- System Description – A short description of the system
- System Utilization – The application of the system
- Systems Strengths – Positive attributes of the system
- System Weaknesses – Negative attributes of the system

Table 41 - Identification Systems

Identification Systems	System Description	System Utilization
Photographic Badge System	Manual production of ID badges. Photograph taken, developed, cut and installed in badge	Low cost, low security Identification
Computerized User Database	Computer system with database to register system users and save user data	Used in conjunction with manual photo or electronic image / biometrics systems
Electronic Image Badge System (EIBS)	Electronic picture captured into computer database	Provide universal biometrics - User Image
Biometrics Badge System	Additional biometrics data collect into computer system	Biometrics registration of user - can include in addition to picture: fingerprints, iris scan, retinal scan, voice print, hand geometry, and signature.
Stand Alone Badge System	Combines computer database with image and possibly biometrics data	Integrated self-contained single station system
Networked Badge System	Badging Issue clients with central database servers	Multiple badge issuing stations
Integrated Badge System	Badge system data is sent to the Access Control System and other systems	Integrates authorized and badged users with access control system and other systems

Table 42 –Identification Systems Strengths and Weaknesses

Identification Systems	System Strengths	System Weaknesses
Photographic Badge System	Low tech	Easy to counterfeit, manual control, labor intensive, no computer data search, eventual disappearance of instant film supplies
Computerized User Database	Provide a searchable database of registered system users	Requires computer, database, power back up, and system training
Electronic Image Badge System (EIBS)	Electronic record of register user's image is saved and retrievable	Requires imaging device, support equipment (tripods, lights, etc.) database for storage of non-text data, and user training
Biometrics Badge System	Adds a verifiable characteristic to user data file	Additional expense and training for biometrics system, weakness of some biometrics systems
Stand Alone Badge System	Inexpensive and simple computer systems	Doesn't allow multiple badge issue stations or shared database
Networked Badge System	Expandable database of system users, enables interface to other systems	Need network connectivity to all badge issue station to central database server, special provision required for off line systems resynchronized to master database
Integrated Badge System	Duplication of data entry of authorized users into ACS not required, allows automated update of user authorization changes, supports adverse termination and real time new user additions, support interface to other systems such as Human Resource, Training, Safety, Legal, etc.	Database for ID systems and other systems must be continually updated and synchronized, System vendors attempt to sell same brand ID and ACS system, database synchronization and coordination issues

3.7.3 Costs

In order to determine overall system costs, the selection of the type and scale of the badging system must be determined. The determining factors for the type of systems are the number of badges to be issued and the geographic location of the personnel that will receive badges. Vendor or expert support can help define transit agencies requirements.

Table 43 provides a summary of costs. Please note that even though materials costs are similar throughout the US, labor costs vary as much as 3 times and this will affect the amounts shown in the tables. Each authority will need to include this factor in implementation and support of the deployed systems.

- Identification System – A list of the types of lighting system
- Cost of Implementation – Range of installing system
- Cost of Maintenance – including operational costs expressed as a yearly % of implementation
- Cost of Training – extra or special training expressed as a one time % of implementation
- Life Expectancy – System life expectancy in years

Table 43 - Identification System Cost

System	Rough Cost of Implementation	Comments	Cost of Maintenance & Operation % per year	Comments	Cost of Training % one time	Commen
Photographic Badge System	$500 to $2K	Obsolete Technology	50 -100%	Film Supplies expensive, dependant on badge production	25%	Procedures, operation, ba production
Computerized User Database	$2 to $5K	Includes computer system & data base software	10-20%	Software costs included in system maintenance, Operator data base update	25%	Data base en procedures a data back up
Electronic Image Badge System (EIBS)	$2K to $25K	System varies from Digital Camera / Computer / Ink Jet printer with basic software to system with badge printer ($6K)	15-25%	Badge supplies (see below), Badge printer ribbon or printer ink, dependant on badge production	25%	Badge produ procedures & printer maintenance
Biometrics Badge System	$2K to $5K	Added cost for Biometrics Registration System	< 5%	Requires cleaning	50%	Thorough tra required to e proper regist
Stand Alone Badge System	$3K to $30K	Stand Alone Workstation or Workstation for Networked system, includes data base and EIBS	25-45%	See above - Computer Data Base & EIBS	-	See above - Computer Da Base & EIBS
Networked Badge System	$4K to $25	Network System includes file server, network interface, and advanced data base, network not included	5-20%	System operator maintenance	0%	Uses existing support syste
Badge Supplies	-	Price vary widely by quantity and security options (Holograms, overlay, custom art work / printing)	-	-	-	-
PVC Plain	$0.10 to $0.50	Price each	n/a	n/a	n/a	n/a
PVC Magnetic Stripe	$1 to $2	Magnetic Stripe type changes price	n/a	n/a	n/a	n/a
Proximity Card	$3 to $5	Passive RFID card	n/a	n/a	n/a	n/a
Contact Smart Card	$8 to $15	Memory capacity changes prices	n/a	n/a	n/a	n/a
Contact Less Smart Card	$10 to $20	Memory capacity changes prices	n/a	n/a	n/a	n/a

3.7.4 Other Factors

There are other factors that must also be considered in the implementation of an identification system. These include, but are not limited to the following.

- Procedures and method for badge issuing must be created and supported
- A badge look, layout and design must be:
  - Unique and easy to identify (determine use of colors, text, holograms, etc.)
  - Difficult to counterfeit
  - Difficult to duplicate
- Security and privacy control
  - Method to prevent unauthorized badge issue
  - Protection of the identification data base
- The need for a badge issuing area
  - Including secure physical space
  - Computer grade electric power
  - Network connectivity to remote badging systems
  - Network connectivity to access control systems

3.8 DATA FUSION, DISPLAY AND CONTROL SYSTEMS

While the term “Intrusion Detection System” can be used to describe a single, stand-alone system (i.e., a “sensor” unit), it is more often used to describe a complete and integrated system that defines, controls, and displays (see Paragraph 1.3) security areas and intrusion into those areas. As such, no Intrusion Detection System would be complete – or effective - without the capability to collect and merge data from various security-related sensors; digest or de-conflict that data and display it in a pre-defined manner; and permit the subsequent control or manipulation of related response systems. For this reason, it is important to understand a few things about Data Fusion, Display and Control Systems.

3.8.1 Technologies

A single software application, or a suite of applications, usually combined with some level of computer hardware that permits the public transportation security staff to ingest real-time data from a multitude of security-related sensors; merge that sensor data into a cohesive format ("data fusion"); display the results in easy-to-understand terms on high-quality monitors or a "video wall"; and allow the user to retain the capability to exercise transportation system or security control functions through the manipulation of that data.

Table 44 - Data Fusion, Display, and Control Systems

Data Fusion, Display, & Control Systems	System Description	System Utilization	System Strengths	System Weaknesses
The term "Data Fusion, Display, and Control" applies to an extremely wide (and developing) variety of systems or software applications from a widely diverse field of vendors or integrators that cover the complete gamut of data fusion, display and control management. Most of these systems or software applications are similar to the types described and discussed below. Actual systems and software titles, applications and vendors number in the hundreds (if not thousands). Therefore, it is recommended that specific research be conducted by the user to identify the specific system or software application (and providing vendor), which best meets the data fusion, display, and control requirements of that user. (See the four separate data fusion, display, and control system descriptions discussed below)	A software application, or a suite of applications, that permits the user to ingest real-time data from a multitude of security-related sensors, merge (i.e., "data fusion") that data into a cohesive format; display the results in easy-to-understand terms on high-quality monitors; and retain the capability to exercise control functions through the manipulation of that data.	Generally used within a security operations center or watch space on computers running the application. Coupled with high-resolution color display monitors, and incorporating carefully tailored and defined security "zones", these data fusion, display, and control software applications streamline security operations.	Primary strength is the manageable fusion of data from disparate sensor systems into a format usable by the security professional. Numerous secondary strengths include reduction of software cost (multiple software titles not required); reduction of manpower requirements; and improved security operations.	Can be difficult to find the right data fusion, display, and control software applications to meet a particular facility's requirements. Many applications focus just on certain systems, such as camera systems, or magnetic sensors, as opposed to multiple sensor types. Frequently not "scalable, i.e., can require upgrades or addition of non-compatible software applications when adding or upgrading overall security sensors.

3.8.2 Applications

A common term used within the military is **C**ommand, **C**ontrol, **C**ommunications, **C**omputers and **I**ntelligence (C4I). All of these capabilities come into play in an effective Data Fusion, Display, & Control System. The level of application involved with any one of these capabilities is entirely driven by the level of security protection desired by a respective transportation facility, the number of sensors being monitored and the number of display workstations in use. Additional examples are provided in table 44, shown above.

3.8.3 Costs

Costs for an effective Data Fusion, Display, & Control System are difficult to estimate because of the large number of determining factors (variables) that control the cost of such a system. The size and type of the transportation facility; the degree of security protection required by the facility or system; the level of system sophistication required by the security staff; the number of IDS sensors and subsystems that must be monitored or displayed; and the degree of communications required - all of these factors (and more) contribute directly to the final cost of a Data Fusion, Display, & Control System. A Physical Security Survey would have to be conducted and overall security system requirements established for a transportation facility before an accurate cost estimate could be developed. Overall costs for an effective Data Fusion, Display, & Control System can range between several thousand dollars to hundreds of thousands of dollars dependent on the above factors. Table 45 provides a summary of costs.

Table 45 - Data Fusion, Display, and Control Systems Cost

Data Fusion, Display and Control System	Rough Cost of Implementation	Comments	Cost of Maintenance & Operation % per year	Comments	Cost of Training % one time	Comments	Life Expectancy
Various Commercial Systems (such as Coastal Surveillance and Display System (CSDS), Security Data Management System (SDMS), and Visual Security Operations Center (VSOC))	Varies	Costs for a Data Fusion, Display and Control System are too wide-ranging to estimate in this table. A cost estimate requires an assessment of a transit facility's requirements.	5 to 10%	Cost based on many factors, including the number of sites & users, and complexity of integrating with existing transit facility sensors and software.	10 to 15 %	Cost based on many factors, including the number of sites & users, the training level desired and amount of travel required by the trainer.	5 to 10 years

3.8.4 Other Factors

There are other factors that must also be considered in the implementation of data fusion, display, and control systems. In order for data fusion, display and control to take place, Data and Power Transmission must be included in the overall initial system wiring and power design and subsequent implementation. Wiring, power and environmental concerns to be considered include the following:

- Cabled Systems – Wire and Fiber Optic
  - Twisted Pair
  - Coaxial Cable
  - Fiber Optic – preferred medium of data transmission
- RF Systems - how vulnerable?
  - Various radio frequency transmission
  - FCC or unlicensed channel
  - Possible interference and jamming
  - Possible interception
- Required Signal Bandwidth - who provides and at what level? Cable or phone line?
  - Low for binary signal
  - Moderate for control signal (example camera pan/tilt/zoom)
  - High for video
- Power Requirement - how much electrical power is needed?
  - Low for data
  - Medium for control (example – camera pan/tilt/zoom system)
  - High for lighting
- Power Systems - what type of power system is in use?
  - Utility Power
  - Emergency Power (on site back up)
  - UPS (4 hours if no Emergency Power, 20 minutes otherwise)
- Transmission Architecture - what type of architecture will be used?
  - Point to Point
  - Multiplex
  - Network
- Transmission Distance - how far and how will it be accomplished?
  - Repeaters
  - Signal Boosters
  - Equalization
- Security - what level will be required?
  - Encryption
  - Physical Protection
  - Line Supervision
- Back Up - what emergency spares will be kept on-hand?
  - Redundant Links

    - Spare Cables
    - Other Spare Parts
- Environmental - what role (if any) will the local weather play in the security system?
    - Temperature extremes (high and low)
    - Weather (rain, snow, icing, flooding etc.)
    - Physical (topographic conditions)
    - Lightning and Transients (electrical grounding)
    - Seismic events (earthquakes)

In addition to the above wiring, power, and environmental concerns, actual system hardware must also be considered, including computer systems, network servers and routers; small and large screen display systems, including "video-wall" systems; and all related alarm display panels or communication networks.

3.9 CRISIS MANAGEMENT SOFTWARE

3.9.1 Technologies

The term "Crisis Management Software" applies to an extremely wide (and developing) variety of software applications from a widely diverse field of providing vendors or integrators that cover the complete gamut of crisis management. Most of these software applications fall into one of the six primary crisis management software categories that are described and discussed in Table 46. Frequently, crisis management software packages will cover most potential crisis or hazard situations in a general way. Some "tailoring" of the software may be required for the facility.

Actual software titles, applications and vendors number in the hundreds (if not thousands). In addition, hundreds of companies exist that will custom tailor either existing software to a requirement, or create a custom software package for a specific or unique requirement. Therefore, it is recommended that research be conducted to identify the specific software application (and providing vendor) that best meets the crisis management requirements of a user.

Table 46 - Crisis Management Software

Crisis Management Software	System Description	System Utilization
Crisis Management Software (See the separate software category descriptions discussed below)	A software application, or suite of software applications, that allows a First Responder, Scene Commander, Crisis Manager or other emergency response personnel to adequately manage and or mitigate an emergency or crisis situation.	Software is pre-installed in reliably backed-up mainframe, desktop, laptop, notebook or personal data assistant (PDA) computers. An initial training session upon software installation and startup is conducted for all appropriate emergency personnel, along with regular refresher training sessions being conducted for designated personnel. Ideally this all takes place prior to the actual occurrence of any crisis event. This applies to each of the six applications listed below.
Emergency Management Software	A software application, or suite of software applications, that allow a First Responder, Scene Commander, Crisis Manager, or other emergency response personnel to adequately manage and/or mitigate an emergency or crisis situation.	
Business Continuity Software	A software application, or suite of software applications, that allow a First Responder, Scene Commander, Crisis Manager, Business or Financial Managers, or other emergency response personnel to adequately manage and/or mitigate a corporate or facility business during or after an emergency or crisis situation.	
Disaster Recovery Software	A software application, or suite of software applications, that allow a First Responder, Scene Commander, Crisis Manager, or other emergency response personnel to adequately manage and/or mitigate damage or injuries while restoring order during an emergency or crisis situation caused by a disaster - natural or otherwise.	
System Backup or Restoration Software	A software application, or suite of software applications, that allow the First Responder, Scene Commander, Crisis Manager, Information Technology (IT) Manager, or other emergency response personnel to adequately manage and/or mitigate an information technology-related emergency or crisis situation.	
Environmental, Health, and Safety (EH&S) Software	A software application, or suite of software applications, that allow a First Responder, Scene Commander, Crisis Manager, EH&S Manager, or other emergency response personnel to adequately manage and/or mitigate environmental, health, or safety-related damage or injuries during or after an emergency or crisis situation.	
Vulnerability Assessment (VA) Software	A software application, or suite of software applications, that allow site management or emergency planning personnel to adequately assess a facilities' vulnerability due to natural disaster or intentional assault PRIOR to the onset of an emergency or crisis situation.	

Table 47 - Crisis Management Software Strengths and Weaknesses

Crisis Management Software	System Strengths	System Weaknesses
Crisis Management Software	A properly installed and managed "crisis management system" (software application and hardware system) provides users with a reliable and easily accessed and display database assets. The system would include emergency plans, available personnel, required material and expected reference material. This applies to all six applications listed below.	Requires a strong management support to develop an adequate overall crisis management software program and to maintain quality software and hardware assets. It needs preliminary and follow-up personnel training. Any shortfalls in the installation or use of the related software application constitutes a weakness (or potential system failure) in the overall program.
Emergency Management Software	Assists in both real time management and post event analysis.	Must overcome user resistance to new workflow and data entry methods.
Business Continuity Software	Enables a business to maintain cash flow.	May impact normal non emergency operations
Disaster Recovery Software	Provides a check list for recovery	System must be carefully crafted to match recovery requirements and must be updated regularly.
System Backup or Restoration Software	Allows quick recovery of IT and related systems.	Backup procedure may not be followed. Data back up may be corrupted
Environmental, Health, and Safety (EH&S) Software	Tuned to EH&S requirements	Complex and sometime not consistent with other systems.
Vulnerability Assessment (VA) Software	See additional data in Chapter 4.	Weaknesses in application can seriously impact a facilities' ability to properly plan for, or mitigate, potential damages or injuries due to an emergency or crisis situation

3.9.2 Applications

A few of the general categories of crisis management include Emergency Management, Business Continuity, Disaster Recovery, System Backup or Restoration, and Environmental/Safety software. Most Crisis Management software will fall into one of these categories. Some software applications may be included as part of a larger hardware system procurement and be more specialized. For example, a large scale Access Control System will also include system management software that may include one or more crisis management applications. In general, it can be said that Crisis Management Software is software that when combined with a related hardware system, assists the user in dealing with unplanned or unexpected intrusions, emergencies, or incidents that threaten a facility's operations, personnel, or physical assets.

3.9.3 Costs

As is typical with most software applications, the purchase, implementation, training and maintenance costs associated with Crisis Management Software can vary widely depending on many factors. It is very difficult to estimate these software costs beyond providing the wide range of between a few hundred dollars per single user-license for a simple application - up to several hundred thousands of dollars for a complete software application support package that includes multiple users, on-site training, follow-on support, future upgrades, etc. Software costs also depend on whether the software is government or commercially developed and marketed; the level of application complexity; the number of licenses and user-copies required; the level of any custom software adaptation that may be needed; and the degree of software implementation training or follow-on support that may be required. It is required that a Physical Security Review be conducted at the transit facility to establish software and data requirements, and for an accurate Crisis Management Software cost estimate to be developed.

Table 48 - Crisis Management Software Cost

Type of Software	Rough Cost of Implementation	Comment	Cost of Maintenance & Operation % per year	Comment	Cost of Training % one time	Comment	Life Expectancy
Emergency Management	Refer to Paragraph 3.9.3	Costs for this type of software is too wide-ranging to estimate in this table. A cost estimate requires an assessment of a transit facility's requirements.	Refer to Paragraph 34.9.3	Cost based on many factors, including the number of sites & users, and complexity of integrating with existing transit facility software.	10 to 20%	Cost based on many factors, including the number of sites & users, the training level desired and amount of travel required by the trainer.	Computer system life
Business Continuity	Refer to Paragraph 3.9.3		Refer to Paragraph 3.9.3		10 to 20%		Computer system life
Disaster Recovery	Refer to Paragraph 3.9.3		Refer to Paragraph 3.9.3		10 to 20%		Computer system life
System Backup or Restoration	Refer to Paragraph 3.9.3		Refer to Paragraph 3.9.3		10 to 20%		Computer system life
Environmental, Health, and Safety (EH&S)	Refer to Paragraph 3.9.3		Refer to Paragraph 3.9.3		10 to 20%		Computer system life
Vulnerability Assessment (VA)	Refer to Paragraph 3.9.3		Refer to Paragraph 3.9.3		10 to 20%		Computer system life

3.9.4 Other Factors

There are other factors that must also be considered in the implementation of crisis management software. These include, but are not limited to the following:

- Software configuration management within the public transportation facility system, and whether it is managed at the city, county, state, or federal level
- Compatibility with other software currently in use both internal (local) and external to the facility (with city, county, state, or federal systems)
- Future software scalability, upgrades, and maintenance
- Requirements for initial and follow-on user training

3.10 OTHER SYSTEMS

This section contains of list of technologies and systems used to provide a complete security solution. These are systems that are different in scope from the Intrusion Detection Systems and supporting access control systems, which is the primary subject of this report. Not all systems listed are required for all transit agencies, and in some cases, additional systems may be required.

Table 49 provides a list of the systems that are not addressed in more detail in this Handbook.

Columns are as follows:

- System Name – Common name for system
- System Description – Brief description of system
- System Utilization – How system is used and area of application
- Comments – Addition comments

Table 49 - Other Systems NOT Addressed

Systems NOT Addressed	System Description	System Utilization	Comments
Asset Tracking Systems	Including Keys, Cards, Security Tokens	Safety and Security	Prevent security breaches by lost keys and other access devices
Computer Security	Firewalls and update software and hardware systems	Safety and Security	Prevent hacker, crackers, and inside jobs
Back Up Data Transmission Systems	Cable, RF, Fiber Optics	Method and means to send security and safety signals and data throughout enterprise	Need back up, recovery plans, and alternative routes
			Follow on to events discussed in the contingency plan
Document Protection & Destruction	Protection and intentional destruction of documents and records	Methods to store paper documents	To prevent unauthorized use and distribution. Need legal input
Drug / Substance Abuse	Checks on personnel, full-time, part-time, temporary, contractors, and visitors	Safety and Security	Need legal and Human Resources input
Facility "Hardening"	Strengthening of primary supports and installation of improved exterior Facility doors and windows	Safety and Security	Steel support beams, doors and shatter-proof windows to mitigate personnel injuries and improve bombing survivability
Fire & Life Safety	Integrate Fire and Life Safety into security system design	Safety and Security	All security systems must comply with local/state/Federal fire codes
Personnel or Background Checks	Checks on personnel, full-time, part-time, temporary, contractors, and visitors	Safety and Security	Prevent "inside jobs"
Power and Power Supplies	Electrical power to operate security systems	Power to all security systems	Need back up, recovery plans, and alternative supplies and sources
Power Back Up Systems	Batteries, UPS, standby electrical power diesel generators	Provide power for continuous system operations	Needed for all computer, video, access control, and IDS systems
Toxic Sensors	Sensors to detect nuclear, radiological, chemical, and biological contaminants	Sensing of contaminants	Expensive and exotic technologies required for effective detector, consulting expertise required for proper selection and application
Training (Periodic, Special, and Emergency)	For all personnel, full-time, part-time, temporary, contractors, and visitors	Safety, Security, and efficiency	Applies to operations, maintenance, and repair
Vehicle Inspection	Methods to inspect vehicles (car, trucks, buses, etc.) for explosives and toxic material	Sensing of contaminants	High to Low tech solutions: Hand inspection, mirror, X-ray, Gamma Rays, dogs, electronic sensors, etc.

CHAPTER 4. Steps in Application and Implementation

4.1 OVERVIEW

This chapter provides checklists and information for the technical personnel in transit agencies on applying Intrusion Detection Systems (IDS) and Access Control Systems (ACS) technologies for securing their facilities. The first sections describe general application steps, with later sections providing data on IDS technology systems. Some data is repeated from Chapter 3 to enable this chapter to stand alone and also to avoid skipping back and forth in this Handbook to look up specific system information. It is important to note that IDS (and related ACS) is only a part of the implementation of an overall security plan for transit facilities.

4.2 APPLICATION STEPS

Listed below are suggested steps to create an effective and optimal Intrusion Detection System for public transit facilities. These sequential steps need to be followed before the effective application and implementation of IDS / ACS security technology.

A full description of the following steps is beyond the scope of this document, so only a short description is included. Numerous technical sources and professional support are available to complete these steps.

4.2.1 Steps Prior to Application of IDS and ACS

A. Identify a Comprehensive List of Assets

This step involves an on-site survey of the proposed security area to compile a list of all system assets. The compiled list of agency critical assets should then be studied to determine the most vulnerable assets, including identifying those that would require protection.

B. Identify Threats to the Assets

Identification of threats to transit assets is a difficult and complex process. The method includes the collection of data on any and all people or groups that may pose a threat to the transit system's assets. Threats run the range from inadvertent intrusion, to juvenile pranks, criminal acts and up to terrorist attacks. Sources for threat information normally include law enforcement at all levels of government (include historical data), data on foreign threats, and other intelligence sources.

C. Identify Vulnerabilities to Assets

Once the assets are identified and the threats summarized, a Vulnerability Assessment can be conducted. During this step, the transit system, in cooperation with others such as law enforcement officials and emergency responders, should determine those assets that are most critical to the agency and that require protection. This assessment produces a

document that identifies the list of critical assets that the transit system needs to protect from identified risks.

D. Assess the Risk and Consequences

The previous three steps are combined into a matrix that summarizes the risk to the Transit Authority. This risk is relative and can change with the introduction of new threats and information. This step also includes consequences of damage or destruction of a facility.

E. Determine Priorities

Limited resources are a reality for all transit systems. By using Risk Assessment data an ordered list of priorities can be set. This list can be ordered by types (for example tunnels) and by consequence (a parts warehouse vs. a heavily used tunnel or bridge). Normally a matrix is generated that includes the methodology of weighing priorities so that the list can be quickly revised with the introduction of new data.

4.2.2 Steps in Applying IDS and ACS

After the completion of the above steps, the process of applying IDS and ACS begins as described below. Details of these technologies are provided in Chapter 3.

The implementation of these systems also follows a sequence of steps. The following lists provide a straightforward approach to implementation of IDS and ACS.

A. Design Criteria

1. Determine facility significance
2. Determine economic loss from intrusion
3. Determine acceptable economic loss
4. Determine intruder's capabilities
5. Determine capabilities of response force
6. Determine characteristics of IDS currently installed
7. Determine force response time (aids in determining system design)
8. Determine security requirements from above
9. Determine optimal trade off of security capital costs versus response force versus operational costs

B. General Design Points

- IDS is installed for two purposes
  - Deter or delay the entry of unauthorized personnel by barriers
  - Provide notification to security forces of unauthorized entry by sensor systems
- Coordinate the design with security forces
  - Robustness of barrier design can increase protection and delay entry time
  - Method of quick alarm assessment must be included

- Barrier delay and alarm notification must be coordinated with security response time

C. Application Steps

- Collect all data from asset identification, threat assessments, vulnerability assessments, risk assessments, and priority settings
- Produce/procure maps of the facility to be protected
- Conduct an on-site survey (see details below)
- Indicate zones and areas of security on the map
- Set security zones as unbroken and enclosed
- Produce layered approached of multiple zones for the best results
- Design from the inside to outside
- Utilize and include existing physical characteristics and infrastructure
  - Existing barriers and fencing
  - Terrain and ground contours
  - Civil structures – roads, building, windows, important rooms, etc.
  - Existing lighting
  - Existing power
  - Existing data and communication networks
  - Existing environmental controls
- When possible place barriers inside IDS alarm zone
  - Provides an alarm before entry into secure area
  - Minimizes damage to barriers
- ACS needs to be coordinated with IDS to suppress nuisance alarms
  - Authorized access suppression of IDS alarms
  - Work versus off-shift alarm suppression
- Lighting work must be coordinated to provide efficient assessment
  - Lighting levels for deterrence
  - Lighting levels for assessment by security workers
  - Lighting levels for video assessment
- A method of alarm assessment must be included
  - Identification of alarm type (intrusion, false, nuisance, environmental)
  - Prioritization of alarm response
  - Ideally a sensor alarm will automatically call up a video image of alarmed area
- Interior sensors versus Exterior sensors
  - Interior sensors are lower in cost
  - Interior sensors are subject to lower problematic alarms (false and environmental)
  - Interior sensors are closer to protected asset so response time is less
- Barriers must be coordinated with health and safety
  - Emergency exit by personnel
- Emergency response entry into area

D. Design Steps -Site Survey

A site survey consists of the confirmation of all available documentation and the collection of actual field data via a survey. This work should be conducted by a team, of at least two people, and extensive images (photo/video) and notes must be taken.

- Field notes – with details and observations
- Identify mismatches between documentation and field conditions
- Note special or unusual conditions
- Take digital photo images (a must)
- Take a high number of digital photos, two pictures of the same view are better that none
- Video tape (optional)
- Note picture direction on area map
- Indicate in field notes any special reason for image
- Interview personnel responsible for operations, management, and security
- Note any existing IDS and ACS

E. Design Plans

The design plan used for the implementation of the IDS, combines all of the following data:

- Threats, Vulnerability, Identification, Risk, and Priorities reports
- Site Survey Report – generally in this format
  - Introduction
  - Purpose
  - Survey Personnel
  - Security requirements
  - Site Description
  - Existing Systems
- Design Criteria
- IDS / ACS operational characteristics (Applicable Technologies)

The plan includes the follow parts:

- Site Plan
- Overall System Block Diagram
- Command Center locations
- IDS Zones
- IDS Barriers
- IDS Sensor Block Diagram
- IDS Sensor Locations
- Lighting Block Diagram
- Lighting coverage zones and locations
- CCTV Block Diagram
- CCTV coverage zones and locations
- ACS Block Diagram

- ACS Locations
- Power support for systems
- Emergency and UPS power for systems
- Communication support for systems
- Temperature control for systems (e.g., Command Center AC)

F. Other Considerations

Environmental influences must be considered in the systems design. Some factors include:

- Temperature
- Rain/Snow/Sleet/Hail
- Frost and Dew Point
- Sun angle (for cameras)
- Vegetation and Trees (blocking view and contribution to environmental alarms)
- Lighting
- Water build up and drainage
- Bodies of water
- Flood
- Fire
- Hurricanes
- Tornadoes
- Earthquakes
- Tsunamis
- High Surf
- Sand Storms

Other factors must to be considered:

- Electromagnetic/Radio Frequency Interference (EMI / RFI)
- Material Storage (blocking view)
- Overhead power lines
- Underground utilities
- Ditches, roads, walls,
- Construction (particularly trenching)
- Power interruption
- Communication interruption

4.3 IMPLEMENTATION OF SPECIFIC TECHNOLOGIES

Intrusion Detection Systems (hardware, software, methods, management, and procedures) are reviewed in the previous parts of this Handbook and form the core of any effective security solution. These systems range from low (simple) technology to more complex (sophisticated) high-technology systems and directly support the prevention and/or detection of intrusion into secure areas.

This section provides specific guidelines to the application of IDS technologies and includes checklists for the actual implementation of these security systems. Once the understanding of security technologies is gained through use of this data, a transit agency will be ready to implement improvements to their intrusion detection systems. Note that there are no established standards that must be followed in every case. The actual order of implementation is often driven by a transit facility's local security architecture, overall security requirements, or direction from higher authority. Sometimes emphasis on a particular security technology area is in response to a specific incident or an identified weakness in that area. Accordingly, the following comments are advisory in nature:

Following the steps above, a plan with a defined security area will be generated, showing the physically defined limits of the area to be secured and indicating the level of required security.

4.3.1 General Implementation Order

The steps for implementation follow the following general order.

A. Define Area and
- Implement Fencing Systems
- Implement Barrier Systems

B. As appropriate, implement the following systems to provide adequate viewing of the secured areas:
- Implement Lighting Systems
- Implement Video Systems

C. Once the area is defined, physically secured, and viewable, the following steps can be applied. The systems identified provide a method to control access to an area by identifying authorized personnel (or vehicles) and allowing movement inside and across secure area boundaries. Sensor systems provide the needed monitoring of this access and movement.
- Implement ACS (see below)
- Implement Sensor Systems
- Implement Identification Systems – proof of identification of authorized personnel

4.3.2 Fencing Systems

Application:
In general, Fencing Systems come in many types, sizes, colors, and materials. These include standard chain-link; woven wire mesh; welded wire mesh; induced pulse ("electrical"); and ornamental fencing, with several types of "topping" options such as barbed wire, razor wire, and rotating spikes. Materials include vinyl, plastic, aluminum and steel. The various fence systems perform several functions, including:

- Provide security perimeters around facilities, buildings or high-value assets
- Provide a clear boundary line between "open" and "secure" areas
- Serve as clear lines of demarcation for security and property lines
- Frequently serve as successful "psychological" barriers to intrusion

- Inhibit or prevent unauthorized entry into designated areas
- Channel or direct the flow of pedestrian or vehicle traffic

Basically, the steps for selecting and implementing security fencing are simple and follow common sense:

- Determine the area around a facility, building, or high-value asset to be secured
- Determine the level of security that is required (low, medium, or high)
- Determine whether the system installation will be temporary or permanent
- Select an appropriate fence type to meet the requirement (style, height, length, etc.)
- Determine whether a fence "topping" is required (barbed wire, razor wire, rotating spikes, etc.)
- If so, select the type of fence top option to be utilized
- Select a fencing contractor and have the fence installed

Checklist:

- ☐ Does the fence meet the transit agency's established security requirement?
- ☐ Does the fence comply with the local building and safety codes?
- ☐ Is the fence-line continuous without any breaks or other areas of vulnerability?
- ☐ Is the fence-line clear of any obstructions inside of 12-feet (minimum) to 30-feet (ideal)?
- ☐ Along the outside of the fence-line, do any nearby objects exist (buildings, electrical boxes, telephone booths, trees, etc.) that could help an intruder intent on climbing the fence?
- ☐ Is the fence properly secured to prevent removal, displacement, modification or theft?
- ☐ Is the bottom of the fence-line secure to prevent climbing under the fence?
- ☐ Is there an adequate degree of security lighting along the fence?
- ☐ If required, are there adequate signs or placards on the fence? In what language(s)?
- ☐ If required, are procedures in place for regular and random security patrols of the fence-line?
- ☐ Are procedures in place for routine inspection of the fence-line and all installed gates?
- ☐ Are there adequate spare parts to support emergency replacement of a failed item?
- ☐ Have the system operators/maintainers/security personnel been consulted or provided input to the selection of this system?
- ☐ If applicable, has user training for this system been arranged through the vendor or provider?
- ☐ Is Point-of-Contact information readily available for the vendor or provider of this system?

4.3.3 Barrier Systems

Application:

In general, Barrier Systems come in many sizes, colors, and materials. Barrier Systems come in two basic types (fixed or deployable) and several styles, including earthen barriers; plain or decorative plastic; metal or concrete "jersey" (K-rail) barriers; concrete or steel bollards; temporary or permanent walls; temporary or permanent "recessed" ramp-style "pop-up" steel barriers; and permanent or quickly deployable portable traffic controllers (steel tire-puncture "teeth").

Barrier Systems perform several functions, including:

- Provide security perimeters around facilities, buildings, or high-value assets
- Provide a clearly boundary line between "open" and "secure" areas
- Serve as clear lines of demarcation for security and property lines
- Inhibit or prevent unauthorized entry into designated areas
- Channel or direct the flow of pedestrian or vehicle traffic
- Provide an impenetrable or crippling barrier to a vehicle attempting to intrude at high-speed

Basically, the steps for selecting and implementing security barrier are simple and follow common sense:

- Determine the area around a facility, building, or high-value asset to be secured
- Determine the level of security that is required (low, medium, or high)
- Determine whether the system installation will be temporary or permanent
- Select an appropriate barrier type to meet the requirement (style, material, height, length, etc.)
- Determine whether a fence "topping" is required (barbed wire, razor wire, rotating spikes, etc.)
- If so, select the type of fence top option to be utilized
- Select a fencing contractor and have the fence installed

Checklist:

- ☐ Does the barrier meet the transit agency's established security requirement?
- ☐ Does the barrier comply with the local building and safety codes?
- ☐ Is the barrier clear of any obstructions within 3-feet (minimum) to 10-feet (ideal)?
- ☐ Is the barrier properly secured to prevent removal, displacement, modification, or theft?
- ☐ Is there an adequate degree of security lighting around the barrier?
- ☐ If required, is there backup power (electrical or hydraulic) to support the barrier's operation?

- ☐ If required, are there adequate signs or placards on or near the barrier? In what language(s)?
- ☐ If required, are procedures in place for regular and random security patrols of the barrier?
- ☐ Are procedures in place for routine inspection of the barrier and related operating hardware?
- ☐ Are there adequate spare parts to support emergency replacement of a failed item?
- ☐ Have the system operators/maintainers/security personnel been consulted or provided input to this system?
- ☐ If applicable, has user training for this system been arranged through the vendor or provider?
- ☐ Is Point-of-Contact information readily available for the vendor or provider of this system?

4.3.4 Lighting Systems

Application:

Lighting Systems consist of numerous components, but primarily the "lighting device" is the main component of interest in this Handbook. These devices utilize a wide variety of methods to generate light and subsequently illuminate a given area of concern. Lighting Systems can be fixed, portable, temporary, or permanent depending on the way that they have installed or utilized. Lighting sources can be incandescent, tungsten, halogen, fluorescent, infrared (IR), mercury vapor, metal halide, high-intensity discharge (HID), low- or high-pressure sodium, and/or several other types. In general, Lighting Systems come in many types, sizes, colors, and degrees of illumination rated in "foot candles" or "candlepower". Light "beams" can be wide-area, narrow-beam ("spot-lighting"), or have a focusing feature for variable beam-width lighting requirements. Lighting Systems generally perform several functions, including:

- Provide lighting for security perimeters around facilities, buildings, or high-value assets in general wide area lighting, spot-lighting, infrared lighting or a combination of several light types
- Provide added element of safety and security by illuminating the workplace
- Provide special illumination (infrared) in support of night-time video surveillance cameras
- Serve as a psychological deterrent ("too well lit…") to intruders
- Inhibit or prevent unauthorized entry into designated areas
- Provide security response forces with added measure of safety by illuminating incident areas (there are hand-carried spot-lights with 6-million candlepower, focus range of 0 to 40-degrees, and a "strobe" feature that can be debilitating to an intruder when aimed at the face)
- Provide temporary or portable lighting for short-term events or emergencies

The steps for selecting and implementing a Lighting System can be complex, but adhering to the following simple steps and using common sense may initially simplify the process:

- Determine the type of lighting system and devices to be utilized
- Determine the area around a facility, building, or high-value asset to be illuminated
- Determine the level of lighting that is required (low, medium, or high)
- Ensure that any lighting system design is compatible with existing video camera systems
- Determine whether the system installation will be temporary or permanent
- Determine the need for portable lighting devices
- Establish the required number of each type of lighting device to be used
- Determine the location of where each light device will be installed
- Ensure adequate electrical service is available to the installation site
- Ensure adequate backup electrical power is available to maintain security lighting
- Determine which light devices will require connection to "emergency power" sources
- Identify an electrical contractor to perform the installation in accordance with local building codes and the National Electrical Code
- Install the lighting fixtures and related hardware

Checklist:

- ☐ Does the lighting system meet the transit agency's established security requirement?
- ☐ Does the lighting system comply with the local building and safety codes?
- ☐ Have lighting effects on neighboring buildings or private homes been considered?
- ☐ Are sufficient portable lighting devices available?
- ☐ Is there a need for specialized spotlighting or infrared (IR) lighting?
- ☐ If required, is there adequate backup electrical power to support the lighting system?
- ☐ Is the lighting system clear of any obstructions within 6-feet (minimum) to 20-feet (ideal)?
- ☐ Is the lighting system properly secured to prevent removal, displacement, modification or theft?
- ☐ If required, are there adequate signs or placards on or near the lighting? In what language(s)?
- ☐ Are procedures in place for routine inspection of the lighting and related operating hardware?
- ☐ Have the system operators/maintainers/security personnel been consulted or provided input to the selection of this system?
- ☐ Are there adequate spare parts to support emergency replacement of a failed item?
- ☐ Is Point-of-Contact information readily available for the vendor or provider of this system?

4.3.5 Video Systems

Application:

Video Systems come with a wide variety of technical capabilities, and in several varying degrees of image quality. These systems include both hardware and software. These capabilities include black and white (monochrome 'B&W'), Thermal (Infrared Sensitive) or color video cameras that range from low-resolution/low-cost daytime cameras (<$100) up to high-resolution/high-cost (>$100,000) "night-vision" thermal-imaging cameras. Software features permit manipulation of imagery; the ability to set "alarm zones" within a visual image; and numerous other functions. Application of the Video System is part of the overall design of the Video System, and for new installations, is best done concurrently with the design of the Lighting System. Video System vendors or technical experts can provide additional and equipment-specific application data beyond the guidelines provided here. Video Systems perform several functions, including:

- Providing a method for remotely monitoring security areas and thus improving security awareness
- Providing a method for initial response and evaluation of observed conditions
- Increasing security force efficiency by allowing quick assessment of intrusion alarms
- Providing a deterrence to intruders by advertising the viewing of suspicious intrusions or activities
- Providing daytime or night-time visual assessment in black and white or color of protected areas around facilities, buildings, fence-lines, or high-value assets
- Preventing unauthorized access into these and other designated areas
- Providing a means for recording of video signals to aid in post-incident analysis, prosecution, or litigation.
- Helping to focus the application of the lighting technologies described above and in Chapter 3

The steps for selecting and implementing an effective video surveillance system can be complex. Adhering to the following basic steps will assist in designing an effective Video System:

- Determine the areas that will require video surveillance
- Perform a survey of the existing lighting systems to ensure sufficient lighting is available
- Determine the number of video systems required for adequate overlapping video coverage
- Identify the video system sites around the facility, building, or high-value asset to be monitored
- Determine the level of security that is required (low, medium, or high)
- Determine whether the system installation will be temporary or permanent
- Select an appropriate video system to meet the requirement (B&W, color, daytime, IR, etc.)
- Determine whether specific video system options (if any) will be required
- Identify a video system and all related hardware and software
- Select a video system contractor and install the system

Checklist:

- ☐ Does the video system meet the transit agency's established security requirement?
- ☐ Does the video system comply with the local building and safety codes?

- ☐ If required, is there adequate backup electrical power to support the video system operation?
- ☐ Have cameras been mounted at an adequate height to provide good field of view (FOV)?
- ☐ Has the camera image format size, lens focal length, and zoom settings been considered for FOV?
- ☐ If applicable, are "IR illuminator" (IR lighting) required for IR imaging camera(s)?
- ☐ Has the rising and setting sun been considered when setting the video camera alignment and FOV?
- ☐ Has a minimum illumination of 2-foot candles throughout the surveillance area been maintained?
- ☐ Have high contrast ratios been avoided in order to prevent video "blooming"?
- ☐ Is an external camera housing (possibly with environmental controls) required for local transit facility conditions (weather, icing, dust, dirt, ocean spray, smoke, etc.)?
- ☐ Is a firm mounting required to prevent motion by wind or the pan & tilt unit movement? This is particularly important to preclude unwanted motion a in higher power camera lens
- ☐ Is the video system clear of any obstructions within 6-feet (minimum) to 20-feet (ideal)?
- ☐ Is the video system properly installed to prevent removal, displacement, modification or theft?
- ☐ If required, are there adequate signs or placards on or near the video system? In what language(s)?
- ☐ Are procedures in place for routine inspection of the video system and related operating hardware?
- ☐ Are there adequate spare parts to support emergency replacement of a failed item?
- ☐ Have the system operators/maintainers/security personnel been consulted or provided input to the selection of this system?
- ☐ If applicable, has user training for this system been arranged through the vendor or provider?
- ☐ Is Point-of-Contact information readily available for the vendor?

4.3.6 Access Control Systems

Application:

ACS provides the method to identify personnel and control entry into secure areas. Interfaces between ACS and the Intrusion Detection System are used to inform the systems to suppress an IDS alarm. This process converts a nuisance alarm “intruder” into an authorized person. Effective integration of ACS and IDS dramatically lower nuisance alarm rates, lower response costs, and prevent the “cry wolf” syndrome (where alarms are so frequent that they are soon ignored).

Not all the steps in the following table apply to all transit agencies or situations. It is permissible to skip steps or provide decisions on some items at a future date. Note that ACS can provide added benefits to business and workflow and is outlined below. These benefits include, but are not limited to time and attendance and training/safety access lock out (for example, personnel with expired training certificate for hazardous work areas can be denied entry).

Table 50 contains the following columns:

- Order – Order to answer questions and provide information. Some items must be answered to proceed to follow on step. Others can be skipped.
- System Characteristic – A short name for data information item.
- Explanation – A short explanation of what the data item is about.
- Information Needed – Data on what information is required. Examples include a count, a map, or list.

Table 50 - Access Control Systems Information

Order	System Characteristic	Explanation	Information Needed
1	Number of Locations	Is this system for one physical location or multiple locations?	List of locations
2	Network Connectivity	If multiple locations, what kind of network connectivity exists between the sites?	Example T-1 data line, or via Internet
3	Area of Containment	Is area enclosed by security barriers? – Fences, Walls, Building, Gates/Portals	Area map with barriers and gates identified for each location
4	System Zones	How many security zones? These are areas of limited access (by time, training, need, etc.)	Defined zones on map
5	Access Rules	Need to determine rules for access to systems zones. A matrix of personnel and business/safety rules that allow access. Example – Chief of Security has full access all the time. Office Janitor has access to public administration building during work hours only.	Full list in matrix form
6	Gates/Doors/Portal	What are the number of personnel and vehicle portals? (Portal = gate, door, etc.)	A count of portals by type
7	Personnel Tracking	Is there a need to know if people are either in or out? Or just secure check in is needed? Secure in & out requires ACS readers on both sides of gate / portal	Secure in & out or just secure in –by location
8	Material Tracking	Is there a need to track vehicles, trucks, computers or other 'materials'?	Yes or no. If yes provide a list.
9	Number of Badges	How many people = number of badges. (Badges = Access Cards)	Count
10	Number of Trackers	If tracking materials is needed, how many?	Count by type
11	Hazardous Conditions	Area card reader installed in hazardous locations?	Limits types of readers
12	Biometrics	Are biometrics used, and if so what type?	Yes or no. If yes what type?
13	Reader Type	What type of reader? Examples – RF Proximity, Biometric	Reader Type
14	Badge Type	What type of badge is needed?	Follow Reader Type
15	Badge Information	What information is needed on badge? Name, photo, employee number, etc.	Graphic of front & back of badge with ALL data
16	Badge Production	Need to determine number & type of badging stations. Input includes number, type, and physical locations	Count & location of badging production stations.
17	Tracker Information	What information is needed on the material tracker 'badge'?	Full description
18	Traffic	How many people use the system on a daily basis?	Number of accesses. In & Out = 2
19	History	How much data is to be saved. Including badges issued, portals transferred, access changes, period of data retention.	Study of traffic to size ACS data storage requirements
20	Data Integration	Does the ACS interface with other systems? Examples include HR, time & attendance, etc.	Data Integration plan with database mapping
21	Intrusion Detection	Is an IDS present? If so what type of integration is required?	Yes or no. If yes list interfaces
22	Video Interface	Is there an interface between ACS and video systems?	Video at portals? Badge photo pop up upon access?
23	Computer OS	Is there a preferred Computer Operating System?	Influence on chosen ACS
24	Installation Support	Is support labor for installation readily available?	In house, contract, turnkey?
25	System Support	Is support labor for maintenance & repair available?	In house or outsource?
26	System Operation	Is support labor available for system operation?	In house or outsource?

Checklist:

- ☐ Does the ACS system meet the transit agency's established security requirement?
- ☐ Does the ACS system comply with the local building and safety codes?
- ☐ If required, is there adequate backup electrical power to support the ACS operation?
- ☐ Is the ACS system properly installed to prevent removal, displacement, modification or theft?
- ☐ If required, are there adequate signs or placards on or near the ACS? In what language(s)?
- ☐ Are procedures in place for routine inspection of the ACS and related operating hardware?
- ☐ Are there adequate spare parts to support emergency replacement of a failed item?
- ☐ Have the system operators/maintainers/security personnel been consulted or provided input to the selection of this system?
- ☐ If applicable, has user training for this system been arranged through the vendor or provider?
- ☐ Is Point-of-Contact information readily available for the vendor or provider of this system?

4.3.7 Sensor Systems

Application:

The choice of sensor system types employed in a particular security solution is largely governed by several related IDS factors listed below:

- Type(s) of Barrier Systems and Fencing Systems
- Type(s) of Lighting Systems
- The field of view (FOV) for the security area of concern
- Cost factors
- The probability of detection (POD) (shown below)
- The probability of environmental alarm (shown below)

Table 51 summarizes the estimated probability of detection for different types of intrusion sensors with relative comparison. Use this table along with the type of fence, barrier, or protection zone to help determine the most suitable sensor. Note that some technologies cannot detect certain types of intrusions; for example, a fence sensor normally cannot detect an intruder bridging over the fence. Note that VH (very high) is the best rating indicated in this table.

Table 51 - Sensor Systems Estimated Probability of Detection (VH is the best rating in this table)

Sensor Systems	Slow Walk	Walk	Run	Crawl	Roll	Jump	Tunnel	Trench	Bridge	Cut	Climb	Lifting
Sensor Lists - Estimate Probability of Detection – very low VL, low L, medium M, high H, very high VH, N/A not applicable	-	-	-	-	-	-	-	-	-		-	-
Binary Sensor	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Buried Sensors												
Balanced Pressure Buried	H	H	H	M	M	M	L	M	L	N/A	N/A	N/A
Fiber Optic Cable	H	VH	VH	VH	VH	H	M	VH	L	N/A	N/A	N/A
Geophone Buried	H	VH	H	M	M	M	L	M	L	N/A	N/A	N/A
Ported Coaxial Buried Line	H	VH	VH	VH	VH	H	M	VH	L	N/A	N/A	N/A
Fence Sensor												
Capacitive Cable	VH	VH	VH	H	H	VH	VL	L	L	H	H	H
Electric Field / Electrostatic Field	VH	VH	VH	H	VH	VH	VL	L	L	H	H	H
Fiber Optic Cable / Mesh	H	VH	VH	VH	VH	H	M	VH	L	VH	H	H
Geophone / Microphone Fence	H	VH	H	M	M	M	L	M	L	VH	H	H
Taut Wire / Tension Sensor	N/A	N/A	N/A	N/A	N/A	VH	VL	VL	VL	H	H	H
Fix Barrier / Wall Sensor	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Infrared Sensors												
Infrared Beambreak Detector	VH	VH	VH	M/H	H	H	VL	L	VL	N/A	N/A	N/A
Passive Infra-Red Sensor (PIR) / Detector (Heat sensor)	VH	VH	VH	M/H	H	H	VL	L	VL	N/A	N/A	N/A
Laser Guard	VH	VH	VH	VH	H	H	VL	M	VL	N/A	N/A	N/A
Microwave Sensors												
Microwave Bistatic	H	VH	H	M/H	M/H	M/H	VL	L/M	L	N/A	N/A	N/A
Microwave Monostatic	H	VH	H	M/H	M/H	M/H	VL	L/M	L	N/A	N/A	N/A
Other Sensors												
Dual Technology Passive IR/Microwave	VH	VH	VH	M/H	H	H	VL	L	L	N/A	N/A	N/A
Magnetic Anomaly Detection (MAD)	H	VH	H	M	M	M	L	M	L	N/A	N/A	N/A
Sound Sensors	L	M	M/H	VL	L	M	M	M	N/A	H	H	M
Video Motion Sensors												
Analog Systems	H	H	H	M/H	M/H	M/H	VL	L	M	N/A	N/A	N/A
Digital Systems	H	VH	VH	H	H	H	VL	L/M	M	N/A	N/A	N/A

Sensors with a high probability of detection may also have the undesired side effect of a higher environmental or false alarm rate. Table 52 lists relative probabilities of environment alarms from different environmental conditions for various sensor types. The type of sensor, along with environmental conditions, must be taken into account when determining the optimal sensor technology. For example, the medium rate for a PIR (Passive Infra-Red) sensor in snow would not be a concern in Miami or in an indoor area. Note that VL (very low) is best rating indicated in this table.

Table 52 - Sensor Systems Relative Probabilities of Environment Alarms (VL is the best rating in this table)

Sensor Systems	Wind	Rain	Standing Water	Snow	Fog	Small Animals	Large Animals	Small Birds	Large Birds	Lightning	OH Power Lines	Buried Power Lines
Sensor Lists - Estimate Probability of Environmental Alarm – very low VL, low L, medium M, high H, very high VH, N/A not applicable												
Binary Sensor	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Buried Sensors												
Balanced Pressure Buried	VL	M	H	L	VL	VL	M	VL	VL	VL	VL	VL
Fiber Optic Cable	M	L	VL	L	VL	L	VH	L	L	VL	VL	VL
Geophone Buried	M	L	L	L	VL	L	VH	VL	VL	M	L	M
Ported Coaxial Buried Line	VL	M	H	L	VL	VL	M	VL	VL	M	VL	L
Fence Sensor												
Capacitive Cable	M	M	VL	M	VL	M	VH	L	M	M	L	VL
Electric Field / Electrostatic Field	M	L/M	VL	M	VL	M	VH	L	M	M	L	VL
Fiber Optic Cable / Mesh	M	L	VL	L	VL	L	VH	L	L	VL	VL	VL
Geophone / Microphone Fence	M	L	L	L	VL	L	VH	VL	VL	L	L	M
Taut Wire / Tension Sensor	VL	VL	VL	VL	VL	VL	L	VL	VL	VL	VL	VL
Fixed Barrier / Wall Sensor	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Infrared Sensors												
Infrared Beambreak Detector	L	L	L	M	M	M	VH	L	M	L	VL	VL
Passive Infra-Red Sensor (PIR) / Detector (Heat sensor)	L	L	L	M	M	M	VH	L	M	L	VL	VL
Laser Guard	L	L	L	M	M	M	VH	L	M	L	VL	VL
Microwave Sensors												
Microwave Bistatic	L	L	M/H	L/M	L	M/H	VH	VL	M	L/M	L	VL
Microwave Monostatic	L	L	M/H	L/M	L	M/H	VH	VL	M	L/M	L	VL
Other Sensors												
Dual Technology PIR/Microwave	L	L	L	L/M	L	M	VH	L	M	L	VL	VL
Magnetic Anomaly Detection (MAD)	M	L	L	L	VL	L	VH	VL	VL	H	M	H
Sound Sensors	H	H	N/A	L	VL	M	H	L	M	VH	L	VL
Video Motion Sensors												
Analog Systems	M	L	L	L	M/H	L	VH	VL	M	L	L	VL
Digital Systems	M	L	L	L	M/H	L	VH	VL	M	L	L	VL

Checklist:

- ☐ Does the sensor system meet the transit agency's established security requirement?
- ☐ Does the sensor system comply with local building and safety codes?
- ☐ Are the proper types of sensors employed and in adequate numbers?
- ☐ Where applicable, have the sensors been calibrated to meet transit specifications?
- ☐ Where applicable, have all sensors that contain high voltage or emit radiation or RF energy been properly identified, labeled, or tagged with the correct warning signage?
- ☐ If required, are there adequate signs or placards on or near the sensor systems? In what language(s)?
- ☐ Is the sensor system clear of any obstructions within 3-feet (minimum) to 10-feet (ideal)?
- ☐ Is the sensor system properly secured to prevent removal, displacement, modification, or theft?
- ☐ If applicable, is there an adequate degree of security lighting around the sensor system?
- ☐ If required, is there backup electrical power to support the sensor system operation?
- ☐ Are procedures in place for routine inspection of the sensor systems and related hardware?
- ☐ Are there adequate spare parts to support emergency replacement of a failed item?
- ☐ Have the system operators/maintainers/security personnel been consulted or provided input to the selection of this system?
- ☐ If applicable, has user training for this system been arranged through the vendor or provider?
- ☐ Is Point-of-Contact information readily available for the vendor or provider of this system?

4.3.8 Identification Systems

Application:

Identification technologies are used to create a credential (usually a plastic or laminated badge) that is used by security personnel and electronic ACS to identify the access authorization of a person or vehicle. These badges use colors, pictures, graphics, and text to identify authorized personnel. A typical badge includes name, digital color photograph, graphics to identify the issuing authority, and additional identification such as prior training and safety data. For electronic access control, an identification method is embedded into the card to allow reading of unique data. This data can include magnetically encoded information ("mag-stripe"), user biometrics template, or a RF "proximity" identification number embedded into a badge.

The steps for selecting and implementing an effective badge system can be complex. Adhering to the following basic steps will lead to effective Identification System design:

- Identify a suitable Identification System type that meets local transit agency requirements
- Determine the number of identification badges that will be required
- Establish the data fields that will be required on the identification badge
- Determine the types of different badge categories (employees, special access, vendors, visitors, escorted, unescorted, one-time entry, multiple entry, etc.)
- Design the layout and look of the badge - usually done by the controlling (issuing) authority
  - Unique and easy to identify
  - Determine use of colors, text, holograms, etc.
  - Difficult to counterfeit
  - Difficult to duplicate
- Establish a method to prevent unauthorized badge issue and methods to protect privacy data
- Establish secure badge issuing areas for protection of the identification data base
  - Must be secure physical space
  - Must have reliable and secure computer-grade electric power
  - Must have network connectivity to remote badge issuing systems
  - Must have network connectivity to ACS
- Determine the Cost of Implementation – Rough range of installing system
- Determine the Cost of Maintenance (yearly operational costs for maintaining the system)
- Determine the Cost of Training for issuing personnel (some minimal level of training may also be required for employee-badge or special access users)
- Determine the required life expectancy of the identification system (usually in years)
- Select a Identification System vendor or expert who can help define transit agencies requirements

Checklist:

- ☐ Does the identification system meet the transit agency's established security requirement?
- ☐ Does the identification system comply with any and all local building and safety codes?
- ☐ Are all procedures in place (and clearly understood) for issuance of identification badges?
- ☐ Are badges to be issued to users in multiple locations?
- ☐ Will these users have access to all of the locations?
- ☐ Will any of these users have "special access" to specially controlled facilities?
- ☐ Are the scanners that read identification system badges clear of any obstructions within 3-feet (minimum) to 10-feet (ideal)?
- ☐ Is the identification system secured to prevent removal, displacement, modification, or theft?
- ☐ Is there an adequate degree of security lighting around the identification system?

- ☐ If required, is there backup electrical power to support the identification system operation?
- ☐ Are procedures in place for routine inspection of the identification system and related hardware?
- ☐ Are there adequate spare parts to support emergency replacement of a failed item?
- ☐ Have the system operators/maintainers/security personnel been consulted or provided input to the selection of this system?
- ☐ If applicable, has user training for this system been arranged through the vendor or provider?
- ☐ Is Point-of-Contact information readily available for the vendor or provider of this system?

4.3.9 Data Fusion, Display, And Control System

Application:

The term "Data Fusion, Display, and Control" (DFDCS) applies to an extremely wide variety of systems and software applications from a diverse field of vendors or integrators that cover the complete range of data fusion, display, and control management. Most of these systems or software applications are similar to the types described in Chapter 3. Actual systems and software titles, applications, and vendors number in the hundreds (if not thousands). Therefore, it is recommended that specific research be conducted to identify the specific system, or software application, or providing vendor that best meets the identified needs for data fusion, display, and control. Generally, these systems:

- Are utilized within a security operations center or watch station
- Are usually coupled with high-resolution color display monitors or "video walls"
- Incorporate monitoring of locally tailored and defined security "zones"
- Streamline security operations by combining all security area visualization, sensor monitoring, and incident response into one display and control system

Checklist:

- ☐ Does the DFDCS meet the transit agency's established security requirement?
- ☐ Does the DFDCS comply with any and all local building and safety codes?
- ☐ Is the DFDCS properly secured to prevent removal, displacement, modification, or theft?
- ☐ If required, is there backup power (electrical or hydraulic) to support the DFDCS operation?
- ☐ If required, are procedures in place for regular and random security patrols of the DFDCS?
- ☐ Are procedures in place for routine inspection of the DFDCS and all related operating hardware?

- ☐ Are there adequate spare parts to support emergency replacement of a failed item?
- ☐ Have the system operators/maintainers/security personnel been consulted or provided input to the selection of this system?
- ☐ If applicable, has user training for this system been arranged through the vendor or provider?
- ☐ Is Point-of-Contact information readily available for the vendor or provider of this system?

4.3.10 Crisis Management Software

Application:

The term "Crisis Management Software" applies to an extremely wide (and continuing to develop) variety of software applications from a widely diverse field of providing vendors or integrators that cover the complete gamut of crisis management. Most of these software applications fall into one of the six primary crisis management software categories listed below:

- Emergency Management Software
- Business Continuity Software
- Disaster Recovery Software
- System Backup (or) Restoration Software
- Environmental, Health and Safety (EH&S) Software
- Vulnerability Assessment (VA) Software

Actual software titles, applications, and vendors number in the hundreds (if not thousands). Therefore, it is recommended that specific research be conducted to identify the specific software application (and providing vendor) that best meets the crisis management requirements of the user.

Once selected, the Crisis Management Software is installed in a reliably backed-up mainframe, desktop, laptop, notebook or personal data assistant (PDA) computer. An initial training session upon software installation and startup should be conducted for all appropriate security and/or emergency response personnel, along with regular refresher training sessions conducted for designated personnel. Ideally this training will take place prior to the actual occurrence of any security-related crisis event

Checklist:

- ☐ Does the software meet the transit agency's established security requirement?
- ☐ Does the software comply with any and all local building and safety codes?
- ☐ Is the software properly installed to prevent removal, displacement, modification, or theft?
- ☐ If required, is there backup electrical power to support the software operation?

- ☐ Are procedures in place for routine inspection of the software and all related operating hardware?
- ☐ Is there an adequate service contract to support changes or upgrades to the software?
- ☐ Have the system operators/maintainers/security personnel been consulted or provided input to the selection of this system?
- ☐ If applicable, has user training for this software been arranged through the vendor or provider?
- ☐ Is Point-of-Contact information readily available for the vendor or provider of this software?

4.3.11 Other Systems (Technologies And Systems Not Addressed)

As discussed in this Handbook, "other systems" consists of numerous security-related technologies and hardware or software systems that are not specifically addressed in this Handbook, but are listed in Chapter 3. The application strategies for these systems should be acquired from the vendor or provider of the particular technology or system, as well as from other transit systems, consultants, or security experts who have had experience with the technology or system.

CHAPTER 5. Management Policies And Procedures

Prior to the attacks of September 11, 2001, many transit systems were already using a variety of intrusion detection strategies. Initially, these strategies were employed to reduce hazards, vandalism and crime; restrict access to secure areas; and raise passenger perceived levels of security when using the transit system. Many of the intrusion detection systems were installed as preventive measures. They were an element in a larger project when buildings were constructed, rehabilitated, or expanded. Others, such as alarm systems placed at parking lots/structures, or barriers at administrative buildings, were installed in response to a specific incident. Generally, these systems have not been modified extensively since they were installed or initiated. In the case of video storage, some agencies have converted from VHS videotape to digital video recorders (DVR). Fences have been repaired, additional cameras and lighting have been installed, and alarm systems have been up-graded. These are the typical system improvements that have been made to intrusion detection systems.

During the course of the project survey (See Chapter 2) and the follow-up interviews, the study team sought to understand the organizations' decision process for selecting the intrusion detection strategies that they are currently using and what their future plans are. The attacks of September 11, 2001, have clearly elevated the priority of security within the transit industry. They have caused some transit systems to implement temporary measures to increase their ability to detect intrusions. Many transit systems have also conducted security surveys to assess their vulnerability to attack and level of preparedness. (For more information on threat and vulnerability analysis, please refer to FTA's *Public Transportation System Security and Emergency Preparedness Planning Guide*, DOT-FTA-MA-26-5019-03-01.) The temporary solutions are candidates to upgrade to a level of permanence, and the findings from the assessments also may result in consideration of new or improved intrusion detection strategies. These new projects have taxed the technical, professional, and financial resources available to the transit systems. In the absence of additional funds being made available to the transit agencies for security related projects, these projects are evaluated for funding against all of the other projects awaiting funding.

As is the case with any project, there are many decision points throughout the project's life. Intrusion detection system projects are no exception. The process begins with the identification of the need. The key issue, once the need has been identified, is how to allocate priorities against the many other pressing requirements at the transit agency. If it is determined that the need is critical enough to address as a project, it will be further defined, and the next series of decision points will be assessed to select and formulate a solution. However, more information may cause a deferment of the project, the implementation of interim solutions, or the abandonment of the project. Limited resources have, in some cases, resulted in decisions to identify and implement quick low-cost upgrades. Assuming that the project is proceeding, the solution(s) have been selected, and vendor supplied products and/or services are required, the implementation approach and procurement methodology become key decisions. These decisions can have a significant impact on cost, schedule, and quality. Implementations can be staged or fast tracked; systems integrators may be used; use of in-house forces, design-build may be an appropriate process to utilize, etc.

5.1 PROJECT TEAM FORMATION

The Project Team responsible for securing the transit system should be a broad based team with a variety of professional skills and perspectives to assist in:

- Defining the problem
- Identification, evaluation, and selection of the solutions
- Implementing the solution/s

Although the scope and magnitude of the project will be the determining factor, the membership of the Project Team would generally be drawn from among the following:

- Operations
- Procurement
- Human Resources
- Engineering
- Security
- Labor Relations

Broad representation on the project teams will insure full consideration of the issues as the projects move forward and increase the likelihood of success. Depending on the type of solutions being considered, it may be of value to also involve the Information Technology function at the transit system. Where necessary, other individuals, with specialized expertise, should be brought in to assist in the effort.

5.2 PROBLEM DEFINITION

The definition of the problem can be determined generally by the security assessments that are being conducted at many transit systems. In some cases, assessments were conducted prior to September 11, and in other cases the attacks of September 11 precipitated a security assessment. These assessments serve to identify the gaps in the current intrusion detection systems. They also identified locations that may be potential targets for a terrorist attack. For example, one transit system had a supply of compressed natural gas to fuel the buses stored at a bus maintenance facility. A detailed security assessment was conducted of the facility and intrusion detection was enhanced significantly with additional fencing, lighting, cameras, and guards. The transit system was not designed with intrusion protection as a design criterion. Some of the short-term remedies that were employed included: fencing (but no razor wire), and new locks. In addition a monthly security assessment of perimeter conditions is now conducted and identified gaps are addressed immediately.

Identify short-term remedial actions - Some of the gaps that have been identified were addressed by some basic low-cost system upgrades. The chief executives that were interviewed strongly recommended that transit systems seeking to upgrade security look for the “low hanging fruit”. These measures could be implemented quickly and generally required little capital investment. In some cases, these measures included the installation of water-filled or Jersey Barriers, the repair of or addition of fencing, new locks, additional lighting, or the assignment of additional law enforcement resources. Security gaps were also found in information technology. Several transit systems found that the Internet contained information and maps on all of the

access points to the transit system. The short-term corrective measure was to secure the non-passenger access and egress points and to concurrently have the information removed from the Internet.

During an interview, a chief executive noted that closing a gap with the deployment of labor might not always be the optimum solution because of the labor costs. The chief executive also indicated that security was not the only concern, "ongoing operations costs are also a concern."

Begin to identify long-term measures - Long-term solutions may entail the use of technology, environmental design, or some other capital investment. It may be the use of technology to reduce the use of manpower to close a gap or enhance the ability to detect intrusions, or the inclusion of increased security measures in the design of a new facility. Other solutions may be the development and implementation of complex procedures and processes, requiring labor negotiations, agreements with other agencies, etc.

As is the case with the short-term measures, financial priorities are a key factor to consider.

Identification, evaluation and selection of the solutions – There are an array of solutions being offered to transit systems to enhance intrusion detection. Some are specific to a particular type of gap. Some have to be modified from the original intended purpose to satisfy the requirements. Others, such as fencing, are directed toward a more general requirement. Most of the solutions involve the use of manpower to varying degrees. Others may only be the implementation of a process or a procedure.

Some of the technologies being offered are very complex and the transit systems may not be familiar with what is available. One chief executive noted that: "Too many vendors with technology show up at the door." Another chief executive expressed frustration over the numerous products being offered that claim to perform a task, but when tested, fail. The chief executive suggested, "The Department of Defense should have a clearinghouse of technologies, thereby saving agencies the time of performing extensive research into potential countermeasures and giving agencies assurance that the technology works." Outside expertise may be required to assist in the evaluation and selection.

There are a number of key considerations in identifying and selecting a solution.

- How well will it work?
- Does it perform as advertised?
- Does it satisfy the need?
- How much will it cost to purchase and install?
- How much will it cost to maintain and operate?
- What supporting or related systems will need to be upgraded or modified, and at what cost?
- How long will it take to implement?
- Is there adequate expertise available to support and maintain the equipment?
- What are the training requirements?
- Are repair and replacement parts available?
- How long will parts be available?

- Will it have any adverse impact on service?
- Is it too labor intensive?
- Are there any labor contract issues?
- Can it be integrated into the existing system?
- Is it compatible with the existing systems?

This represents a sample of the factors to consider. Additional technical and policy considerations will likely be appropriate to accommodate local requirements.

5.3 IMPLEMENTING THE SOLUTIONS

The implementation phase of the project consists of several elements. It includes the preparation of the solicitation, the selection of vendors, and the actual implementation. Prior to the preparation of the solicitation, the optimum implementation approach should be determined. The selected approach will have an impact on the specifications and the form of the solicitation.

Among the approaches that may be considered are:

- Use of an integrator as the prime contractor
- Use of in-house forces to install the technology
- Use some form of a design build or turnkey approach
- Use a fast track implementation approach
- Use a traditional design bid build approach
- Stage the implementation

As is the case with any project, a number of factors influence the implementation approach. These factors include:

- Degree of project urgency
- Funding availability and sources
- Availability of in-house expertise
- Local procurement laws
- Degree of technological complexity
- Degree of project risk
- Desired level of control
- Project schedule
- Availability of contractors and suppliers
- Level of required integration

Once the project approach is determined the procurement can be conducted.

In those cases where FTA funds are used, in whole or in part, to fund the intrusion detection project, the procurement methodologies allowed are contained in Section 9 of FTA Circular 4220.1D. The procurement process can range from a telephone call to a request for proposals or sealed bids. While the FTA Circular provides broad choice and discretion in the procurement methodology, local law usually restricts the method of procurement more tightly than these Federal requirements. Procurement methodologies and considerations would therefore depend

on the type of intrusion detection project, complexity, estimated cost, and applicable procurement regulations that apply to the transit system. Under certain restricted circumstances, a non-competitive proposal from a sole source will be appropriate. In cases of emergencies, as may be the case with some intrusion detection projects, many transit systems are generally permitted, in accordance with Federal and state law, to enter into sole source contracts in those cases where it has been determined that a public exigency exists. Non-competitive proposals from a sole source may also be appropriate in certain upgrade projects that involve proprietary software or systems.

CHAPTER 6. Conclusions

6.1 CONCLUSIONS

Unwanted intrusion into public transportation facilities is an industry-wide problem that affects safety, security, service reliability, productivity, claims, and customer relations. The problem has been approached with a variety of both high and low technology solutions producing a wide range of results. Applications address both prevention and detection and include Access Control Systems (ACS) and Intrusion Detection Systems (IDS). The heightened concern for safety and security in public transportation facilities and vehicles has led to increased investment in both ACS and IDS. At the same time, changing economic conditions have resulted in reduced funding and more scrutiny in capital and operating budgets. This Handbook is intended to assist transit executives, managers, technical, financial, and procurement personnel as they assess the options available for improved access control and intrusion detection.

Strategies to enhance and upgrade intrusion detection invariably employ a combination of measures. They can include procedures/process, technology, building/facility design, and human resources. The likelihood of the success of the implementation of any security related strategy is increased when it is approached with the same discipline associated with a project. Such discipline will ensure that there is a full consideration of the issues and alternatives.

This Handbook contains extensive data on the current state of the practice, available technology, practical steps for selection and implementation, price ranges, and management considerations; however, it should not be considered the only resource to support decisions for access control and intrusion detection. Rapidly changing technology requires that technical staff keep abreast of the latest developments in these areas. Also, public transit professionals at all levels should continue to utilize the various networks of communication that are available to talk personally with other professionals who have current, applicable experiences.

6.2 FUTURE RESEARCH

Transit systems are among the most vulnerable public facilities in the world. Open access and large numbers of users make facilities such as train stations potential targets with catastrophic implications in the case of a terrorist attack. Follow-up research to this Handbook is necessary as the security technologies and system needs are rapidly evolving. Some of the areas for consideration for future research include:

- Conducting a study on current threat-induced airborne chem-bio contaminants. This would also include bio-contaminates such as anthrax, smallpox, etc. The recent cyanide gas threat against the London Underground is an indication of the existing threat.
- Developing guidelines for in-depth Vulnerability Assessments (VA) of high-threat transit facilities.
- Conducting an updated study aimed at transit system application of the most leading-edge security systems research being performed by the nation's top security corporations and labs.
- Conducting further transit system surveys with more in-depth analyses and interviews to expand on what is included in this Handbook

- Establishing and operating a "Transit Facility Security Testbed" wherein various new technologies could be installed at a selected transit site and evaluated for use at other transit sites. A model is the U.S. Navy Testbed for evaluating security and IDS systems for subsequent utilization at all Navy and Marine Corps bases.
- Conducting research on design specific systems for protection of transit facilities. For example, train gates to allow uninterrupted train traffic and to disallow intruders. These systems would be applied to gates and doors to distinguish the authorized users.
- Conducting research for detailed methods and procedures for access and badging (credential) to include layout, design, and implementation.
- Researching integration methods for IDS and ACS.
- Researching methods and procedures for video system integration with IDS.

APPENDIX

A. **Glossary of Terms**
B. **Bibliography**
C. **Literature Review**
D. **Copy of the Transit Agency Survey**
E. **State of the Practice (Results of Surveys, Interview, and Site Visits)**

A. GLOSSARY OF TERMS

Term	Description
Access Control	Methods and technologies used to identify and control access to a defined area. Used in conjunction with IDS to control nuisance alarms
ACS	Access Control System
Alarm Processing	Evaluation of sensor input data to determine whether to annunciation an alarm
APTA	American Public Transportation Association
Area Sensor	Sensor used to monitor a physical surface area such as a floor, outdoor ground area, etc. Ranging from as simple as a pressure mat, to as complex as a buried field sensor. Distinction between Area and Volume sensors are sometimes limited
Balance Pressure Switch	An IDS sensor that alarms when subjected to a pressure differential
Barrier Sensors	Sensors used to monitor a physical barrier - fence, wall, roof, window, etc.
BIA	Business Impact Analysis
Binary Sensor	An IDS sensing device that has only 2 states - open or closed, which is used to annunciate alarms. Example = BMS
Biometric	The utilization of a personal biometric trait to identify a user to ACS and IDS systems. Examples are fingerprints, iris scans, retinal scans, hand geometry
Bistatic Sensor	An IDS sensor that consists of two parts: a transmitter and a receiver. Normally, interruption of the transmitted sensor energy (IR, laser, microwave, etc.) cause an IDS alarm
BMS	Balance Magnetic Switch - A set of contacts and magnets used to annunciate the opening / closing of door, window, or other device. Replaces magnetic position switches that are easily defeated and bypassed.
Breakwire	An IDS sensor that alarms an IDS when a wire or other cable is broken
BCP	Business Continuity Plan
C2	Command & Control
C3	Command, Control, & Communications
C4I	Command, Control, Communications, Computers & Integration - Military term to define an integrated system for overall control and operation of a complex operation
Capacitance	An IDS sensor technology that measures the disturbance of a capacitive field set up to protect fixed objects
CATS	Consequence Assessment Tool Set
CCTV	Closed Circuit Television - Video camera system used to monitor defined area. Imaging includes color, black & white, and thermal sensors.
COTS	Off The Shelf - technologies and solutions that are readily available and do not require development research work. COTS can be configured to specific applications without development or research.
Crisis Management	A set of methods and procedures used to address crisis situations.
CSDS	Coastal Surveillance and Display System
Data Fusion	Methods to collect and display various IDS sensors and systems information
DB	Data Base - also database or dB

Term	Description
DFDCS	Data Fusion, Display, and Control - applies to an extremely wide variety of systems and software applications from a diverse field of vendors or integrators that cover the complete range of data fusion, display, and control management
Dual Technology	IDS sensors that use two methods jointly to sense intrusions. Example is IR & Microwave
Duress Alarm	A binary sensor device activated covertly by personnel to annunciate to an IDS the occurrence of an alarm condition
DVR	Digital Video Recorder - method of recording video signals from CCTV systems by digitizing the analog video signal, compressing, and saving on computer style hard disk storage.
EBS	Electronic Badging System - system that saves a user's picture and other relevant data (including, if required, biometric information) into a database. This information is used to create credentials that are used by guard force personnel and access control systems for both identification & access control.
EECS	Electronic Entry Control Systems - ACS
EH&S	Environmental Health and Safety
EIBS	Electronic Image Badge System
Electric Eye	An IDS sensor that senses to transmission of visible or invisible light
EMI	Electro-Magnetic Interference
Environmental Alarm	Alarm annunciated from environmental condition that mimics an intrusion
False Alarm	Alarm annunciation from no apparent cause
FAR	False Alarm Rate - a rate or ratio of false alarms to other alarm times
Fiber Optic Cable	A cable consisting of glass or plastic used to transmit light (visible or invisible). Alteration or interruption of the light is used by IDS sensors to annunciate intrusion
FOV	Field Of View - used for CCTV systems and defines the angle of viewing of the system (in horizontal and vertical). FOV is controlled by camera image sensor size and lens type and setting.
FTA	Federal Transit Administration
Geophone	An IDS sensor that utilizes sound and pressure to detect intrusions
HASCAL	Hazardous Assessment for Consequence Analysis
HID	High Intensity Discharge
HR	Human Resources
ID	Identification
IDS	Intrusion Detection System
IES	Illumination Engineering Society
Intruder	Unauthorized person, animal, or object in a restricted area.
Intrusion Alarm	Alarm generated by an IDS. Alarms include Intrusion, Nuisance, Environmental, and False. Also an alarm generated by an intruder entering or violating a protected area.
Intrusion Detection	Methods and technologies to sense and annunciate the intrusion of personnel into a defined area.

Term	Description
IR	Infra-Red - Optical wavelength outside normal human viewing, normally above 700 microns. Beyond Red.
LED	Light Emitting Diode
Microwave Sensor	An IDS sensor that uses the disturbance of microwave energy to annunciate an intrusion
Monostatic Sensor	An IDS sensor that consists of one part,with transmitter and receiver mounted in the same physical device
NAR	Nuisance Alarm Rate - a rate or ratio of nuisance alarms compared to other alarm types
Nuisance Alarm	Alarm annunciation from the detection of an intruder that is NOT an intrusion. Example is an authorized worker who enters a protected area with proper suppression of the IDS alarm.
PC	Personal Computer
Piezoelectric	An IDS sensor that uses the physical effect of voltage generation caused by the exertion of pressure on certain materials
PIN	Personal Identification Number - used in access control systems to prevent use of ID badges by unauthorized personnel
PIR	Passive Infra-Red (sensor) - system that used human IR (heat) emissions for detection purposes.
Point Sensors	A sensor that is used to monitor a single point such as door position (open or closed)
Ported Coaxial	An IDS sensor that uses a leaky (purposely designed cable with poor shield) to detect intrusion. A RF signal is injected into the cable and interference of the field produced around the ported cable causes an IDS alarm
Pressure Sensor	An IDS sensor that detects pressure (usually intruding personnel) and alarms when activated
PTZ or P/T/Z	Pan Tilt Zoom - control of camera systems - pan is side to side motion, tilt is up and down, and zoom is FOV adjustment via camera lens control
RF	Radio Frequency
RFI	Radio Frequency Interference
SAIC	Science Applications International Corporation
SDMS	Security Data Management System
Security Screen	An IDS sensor that utilizes a mesh of breakwires to alarm an IDS when open or broken.
Sensor Processing	Equipment and computer processors that receives sensor inputs and determines if an alarm condition exists. Provides binary output of processing decision
TCRP	Transit Cooperative Research Program
TIS	Thermal Imaging System
UL	Underwriters Laboratories
Ultrasonic	An IDS sensor system that utilizes high frequency sound for intrusion detection
UPS	Uninterruptible Power Supply - system used to provide back up power in the event of loss of AC line power. Usually a system of AC to DC and DC to AC converters with a battery supply source.
VA	Vulnerability Assessment - a study to determine potential vulnerabilities to a defined area or system

Term	Description
Video Motion	An IDS sensor system that analyses and compares video signal for the detection of intrusion
VMS	Video Monitoring System - a complete video system including cameras, lenses, camera control, camera and control power, signal transmission, video display, video switching, video control, and video recording
Volume Sensors	Sensor used to monitor a physical space such as a room interior, volume around a door, or volume adjacent to a fence
VSOC	Visual Security Operations Center

B. BIBLIOGRAPHY

1. *A Guide to Highway Vulnerability Assessment and Appendices*, American Association of State Highway and Transportation Officials' Security Task Force under National Cooperative Highway Research Program Project 20-07/Task 151B, May 2002. (http://security.transportation.org/community/security/doc/guide-VA_FinalReport.pdf)
2. *A Guide to Updating Highway Emergency Response Plans for Terrorist Incidents and Appendices*, American Association of State Highway and Transportation Officials' Security Task Force under National Cooperative Highway Research Program Project 20-07/Task 151A, May 2002. (http://security.transportation.org/community/security/doc/guide-ResponsePlans.pdf)
3. *Access Control & Security Systems Buyers Guide - Access Control & Security Systems Volume 45 / Number 6*, 2002.
4. *Access Control Units (UL 294),* January 1987.
5. *Bart Intrusion Detection System With Costing*, December 2002.
6. *Biometrics Explained*, International Biometrics Group, 2001.
7. *Biometrics Technology Overview*, April 2002.
8. *Body Check – Biometrics Defeated*, c't Magazine Germany, June 2002.
9. *Bridge Monitoring for Acoustic Events,* Pure Technology Ltd. - Acoustic Monitoring, June 2002.
10. *CCTV*, Book by Vlado Damjanovski, Butterworth-Heinemann, 2000.
11. *Design Guidelines for Physical Security Facilities (Military Handbook 1013/1A),* October 1987.
12. *Design Manual 13.02, Commercial Intrusion Detection System (ID)*, Naval Facilities Engineering Command, September 1986.
13. *Electronic Surveillance Technology on Transit Vehicles (TCRP Synthesis 38),* Federal Transit Administration (FTA)/Transit Cooperative Research Program (TCRP), 2001. (http://gulliver.trb.org/publications/tcrp/tsyn38.pdf)
14. *Energy Efficient Lighting (DOE / GO 10095-056),* U.S. Department of Energy, December 1995. (http:// www.eren.doe.gov/erec/factsheets/eelight.pdf)
15. *Federal Specification Components for Interior Alarm Systems (W-A-450C),* August 1990.
16. *FPED III CD,* Force Protection Equipment Demonstration III Information CD contains product pages for force protection equipment demonstrated and displayed during FPED III held at US Marine Corps Base, Quantico, Virginia, May 2001.
17. *IDS GEGS 16725,* Army Corp of Engineers, April 1991
18. *Intruder Detection Systems,* London Underground, 1993.
19. *Improving Transit Security, A Synthesis of Transit Practice (TCRP Synthesis 21),* Federal Transit Administration (FTA)/Transit Cooperative Research Program (TCRP), 1997. http:// www.nas.edu/trb/publications/tcrp/tsyn21.pdf
20. *Intrusion Detection Units (UL 634),* July 1993.
21. *Intrusion Detection & Assessment (DOE Order 5632.1C & DOE Manual 5632.1C-1),* U.S. Department of Energy.

22. *Manual For Protection and Control of Safeguards and Security Interests (DOE 5632.1C),* U.S. Department of Energy Office of Security Affairs Office of Safeguards and Security, July 1994. (www.oa.doe.gov/sase/directives/m56321c-1c1.pdf)
23. *Military Specifications Control Electronics (MIL-C-52913),* January 1989.
24. *Military Specifications Monitor Module, Status and Monitor Modules, Alarm (MIL-M-5287C),* February 1986.
25. *National Preparedness - Technologies to Secure Federal Buildings (GAO-01-687T),* Statement of Keith A. Rhodes, April 2002. (http:// www.gao.gov/new.items/d02687t.pdf)
26. *Perimeter Security Handbook,* Defense Advanced Research Projects Agency (DARPA)/ Naval Command, Control and Ocean Surveillance Center, In Service Engineering - East (NISE East), 1997. (http:// www.nlectc.org/perimetr/full2.htm)
27. *Physical Security (FM 3-19.30),* Department of the Army, January 2001. (www.globalsecurity.org/military/library/policy/army/fm/3-19-30/toc.htm)
28. *Physical Security Design, Design Manual (NAVFAC DM – 13.1),* Naval Facilities Engineering Command U.S. Navy, 1983.
29. *Physical Security Systems Inspectors Guide,* U.S. Department of Energy Office of Safeguards and Security Evaluations, September 2000. (http:// www.oa.doe.gov/guidedocs/0009pssig/toc.pdf)
30. *Proprietary Burglar Alarm Units and Systems (UL 1076),* December 1988.
31. *Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices (MTI Report 01-07),* Mineta Transportation Institute, Brian Michael Jenkins and Larry N. Gersten, September 2001. (http://transweb.sjsu.edu/publications/terrorism_final.htm)
32. *Protecting Surface Transportation Systems and Patrons from Terrorist Activities - Case Studies of Best Security Practices and a Chronology of Attacks (IISTPS Report 97-4),* Mineta Transportation Institute, Brian Michael Jenkins, December 1997. (http://transweb.sjsu.edu/publications/terrorism/Protect.htm)
33. *Protecting Surface Transportation Against Terrorist and Serious Crime: An Executive Overview,* Mineta Transportation Institute, Brian Michael Jenkins. (October 2001). http://transweb.sjsu.edu/publications/TerrorismExOverv.htm
34. *Public Transportation System Security and Emergency Preparedness Planning Guide*, DOT-FTA-MA-26-5019-03-01
35. *Security Engineering Electronic Security Design (TM 5-853-4),* Department of the Army, 1994.
36. *Security: A Guide to Security Systems Design and Equipment Selection and Installation,* Book by Neil Cumming, Butterworth-Heinemannm, 1992.
37. *Terms, Definitions and Symbols for Security Equipment and Practices (FED-STD-800),* January 1989.
38. *Transit Security Handbook,* Volpe National Transportation Systems Center, March 1998. (http://gulliver.trb.org/publications/security/TransitSecurityHandbook.pdf)
39. *US Army Corp of Engineers Cost Estimator Electronic Security Systems – Spreadsheet with guide,* U.S. Army Corp of Engineers, January 2001.

Intrusion Detection Related WEB SITES	
ACS	www.casi-rusco.com
ACS	www.lenel.com
ACS	www.swhouse.com
ANSER homeland defense page	www.homelandsecurity.org/research.cfm
Biometric	www.handreader.com
Biometrics	www.biometricgroup.com
Bollards/barriers – including hydraulic	www.deltascientific.com
Business Impact Analysis (BIA) and the Business Continuity Plan (BCP) Generator from Disaster Recovery World	www.disasterrecovery.com
Camera & CCTV	www.panasonic.com/cctv
Camera & CCTV	www.pelco.com
Camera Source Book	www.securitysystemsnews.com
Coastal Surveillance and Display System (CSDS)	www.saic.com
Concrete bollards/barriers	www.stonewear.com
Consequence Assessment Tool Set (CATS)	www.saic.com
Control Electronic Security	www.controlelectronic.com
Defense Data	www.dtic.mil/dtic
Fencing	www.riverdale.com
Fencing	www.cawire.com
GE Lighting	www.gelighting.com
Glossary	www.ciao.gov/ciao_document_library/glossary/F.htm
Hazardous Assessment for Consequence Analysis (HASCAL)	www.ornl.com
Identification Systems	www.datacard.com
Identification Systems	www.identicard.com
Identification Systems	www.lenel.com
Identification Systems	www.casi-rusco.com
IDS	www.optexamerica.com
IDS	www.senstarstellar.com
IDS	www.perimeterproducts.com
IDS	www.safeguards.com
IDS	www.fibersensys.com
IDS	www.southwestmicrowave.com
IDS	www.beicomm.com
IDS	www.rtms-by-eis.com
Induced Pulse Fencing	www.rutland-electric-fencing.co.uk
IR Camera	www.indigosystems.com
IR Cameras	www.diop.com

Intrusion Detection Related WEB SITES	
LED Lighting	www.ledtronics.com
McQ Associates “OmniSense”	www.mcqassociates.com/IDS-Seismic,Magnetic,PassiveIR,andAcousticSensorUnits; ProcessingUnitandDisplayUnit
Mesh Fence	www.metlx.com
Intelligent Tracking Software	www.remotereality.com
Razor Fencing	www.binns-fencing.com
RiskWatch for Physical Security from RiskWatch	www.riskwatch.com
Rotating fence toppings	www.jncfence.com
Secure Technology Inc.	www.securetechnology.com
Security	www.dtic.mil/ndia/security
Security Data Management System (SDMS)	www.vistascape.com
Security Links to Equipment	www.intiss.com/pslinks.html
Sentrol – Now part of GE Interlogix	www.sentrol.com
Taut Wire IDS	www.govcon.com/content/ProductShowcase/product.asp?DocID={93A50FFB-6459-11D6-A789-00D0B7694F32}
US Army Corp of Engineer Support Center	www.hnd.usace.army.mil/techinfo
Visual Security Operations Center (VSOC)	www.vsoc.com

The references in the above table are provided for information purposes only. This Handbook does not endorse any companies or products to provide intrusion detection technologies or devices.

C. LITERATURE REVIEW

The material presented in this Handbook is derived from a careful review of information compiled from commercial, state, federal, and international agencies and their personnel. The information was acquired through telephone calls, emails, a survey, and extensive online research. The objective was to identify, assess, and document the state of the practice in the use of intrusion detection systems in the transit industry.

The online literature search concentrated on intrusion detection technologies such as lighting, fencing, barriers, video cameras, identification systems, access control systems, sensors, security management systems, and crisis management software. Some of the documents found include military manuals, security system inspector's guides, technology handbooks, government reports, and vendor technology reviews. The documents obtained are cited in the bibliography to this Handbook in the appendix.

Much of the literature contained similar information with respect to specific security technologies. Many documents focused on common deficiencies, weaknesses, and potential concerns such as false alarms, improper installation, tamper protection, inadequate testing, and optimum coverage. Also mentioned are the capabilities, limitations, and integration methods of current perimeter security sensor technology. The referenced handbooks provide a compendium of sensor technologies, a general explanation of each technology, as well as integration techniques that can be used to enhance perimeter security and intrusion detection planning.

The references below represent a small portion of findings from the literature search, but provided some of the more relevant background information on intrusion detection and access control systems.

National Preparedness - Technologies to Secure Federal Buildings (GAO-01-687T), Statement of Keith A. Rhodes, 2002. The report discusses commercially available security technologies that provide protection, detection, and reaction capabilities. Evaluations of 12 Access Control Technologies, 3 Detection Technologies, and 2 Intrusion Detection Technologies are provided. Each technology evaluation begins with a picture of the specified technology followed by a general description of how it works. Next is an assessment of the effectiveness and performance factors. The report provides discussion on user acceptance of the technology, describing issues or concerns that some organizations have experienced when implementing the particular system. Also included is a unit price range along with potential vendors of the technology.

Electronic Surveillance Technology on Transit Vehicles (*TCRP Synthesis 38*), Federal Transit Administration (FTA)/Transit Cooperative Research Program (TCRP), 2001. This document focuses on the state of the practice regarding on-board vehicle surveillance technologies. The synthesis begins with system design and a description of existing technology including closed circuit television, event recorders, and audio surveillance. Representative technology configurations from seven transit agencies (Philadelphia, Chicago, Ann Arbor, Milwaukee, Buffalo, St. Louis, and Portland) provide approximate system cost, reasons for use, installation summary, and more. The document also explores the benefits of surveillance technology with the assistance of statistical tables and graphs. The ending chapter addresses three issues that

exist with surveillance technologies on vehicles including financial, legal, and mechanical and procedural.

Physical Security Systems Inspectors Guide, U.S. Department of Energy Office of Safeguards and Security Evaluations, 2000. The guide provides security system inspectors with a set of detailed tools and references that can be used to plan, conduct, and close out an inspection. Appendix A (Intrusion-Detection Systems) of the document includes performance tests for a variety of intrusion-detection systems such as Exterior Perimeter Sensors, Interior Sensors, Perimeter CCTV, Interior CCTV, and Alarm Processing and Display Equipment.

Transit Security Handbook, Volpe National Transportation Systems Center /Federal Transit Agency, 1998. The Handbook provides an overview of the rail security function such as the establishment of a rail transit police or security department, the development of a System Security Program Plan (Security Plan), the deployment of uniformed and plainclothes police and security personnel, Crime Prevention through Environmental Design (CPTED) and Situation Crime. Also included are prevention (SCP) techniques for rail facility design and operation, specifically the use and management of security technology, and techniques for crime data collection and analysis.

Perimeter Security Sensor Technologies Handbook, Defense Advanced Research Projects Agency (DARPA)/ Naval Command, Control and Ocean Surveillance Center, In Service Engineering - East (NISE East*)*, 1997. The Handbook provides military and law enforcement security managers, and specialists with a reference of perimeter security sensor technologies, capabilities, limitations, and integration methods. Sensor technology reviews provide useful information, such as: the operating principle – a simplistic description of how the system works, sensor types/configurations – a description of those systems that have multiple "types", applications and considerations – a description of the recommended environment the specific system is designed for and conditions that may cause unreliable detection or nuisance alarms, and user acceptance of the technology - issues or concerns that some organizations have experienced when implementing the particular system.

Manual For Protection And Control Of Safeguards And Security Interests (DOE 5632.1C), U.S. Department of Energy Office of Security Affairs Office of Safeguards and Security, 1994. The document is composed of 14 chapters that provide detailed requirements for protection of safeguards and security interests. Chapter 6 of the document focuses on intrusion detection and assessment systems. This chapter describes the requirements that an intrusion detection system must meet and maintain with respect to: perimeter coverage, false alarm rates, system testing, lighting, auxiliary power, and intrusion detection system protection.

Each of these documents is available to the public and can be found on the Internet. A complete listing of references is provided in Appendix B of this Handbook

D. SURVEY QUESTIONNAIRE

INTRUSION DETECTION FOR PUBLIC TRANSPORTATION FACILITIES

Your assistance in completing this survey questionnaire will provide valuable information for understanding the current state-of-the-art practices, equipment and resources utilized for intrusion detection for public transportation facilities. The questionnaire is intended to gather information related to intrusion detection applications for any and all public transportation facilities as well as vehicles.

Facilities should include the following:

- Administrative Buildings
- Maintenance Facilities (Bus & Rail)
- Storage Facilities
- Rail Yards
- Operational Control Centers
- Power Stations
- Train Control Areas
- Stations
- Tunnels
- Bridges
- Terminals/Transfer Facilities
- Operating Right-of-Way
- Parking Lots/Structures

Vehicles should include:

- Trains/Rail Vehicles
- Buses
- Service/Support Vehicles
- Special Purpose Vehicles
- Para-Transit Vehicles

Intrusion Detection Applications could include:

- Video Surveillance
- Access Control Systems
- Sensors
- Alarm Systems
- Fences
- Barriers
- Lighting
- Human Resources
- Other

The Survey Questionnaire has twenty-one questions with associated tables to simplify your response. Please follow the instructions related to each question and provide as much additional information as possible on specific items at the bottom of each table. Unless otherwise stated in the question, only provide responses for current intrusion detection applications on existing public transportation facilities or vehicles.

Thank you for taking the time to provide responses to this survey questionnaire. Your time and commitment are appreciated.

1. What type of Intrusion Detection System(s) is currently being utilized? (Please check all applicable boxes)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

2. Is it purely utilized for security? (Please check boxes) Is it also meeting an operating requirement? (Please add a plus sign)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

3. Was the application in response to a specific incident? Was it for purely preventive measures? (Mark I for incident and P for preventive)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

4. Has the application accomplished its intended purpose? (Please mark Y for yes and N for no)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

5. Have you realized any secondary benefits? (Please mark Y for yes and describe below)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

6. Has the application functioned as originally intended? (Please mark Y for yes and N for no)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

7. What modifications have been made since the original installation? (Please check applicable boxes and explain below)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

8. Was the application custom made (mark with C) or off the shelf (mark with S)?

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

9. Have there been any adverse effects on operations or other functions as a result of the application? (Please check for yes and explain below)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

9. If you had to make the same decision today, would you select the same application/product? (Please mark Y for yes and N for no)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

10. What was the full capital cost of the application, including installation? (Please indicate $ amount)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

12. What are the annual costs of operating and maintaining the application? (Please report as a % of total installation cost, and if available, breakout for general maintenance, repair and vandalism)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

13. How reliable is the system based on failure rates and false alarm rates? (Please mark from 1 low to 5 high)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

14. How much maintenance is required on the system? (Please mark from 1 low to 5 high)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

15. What is the life expectancy of the system(s) you currently utilize? (Please indicate the number of years)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

16. Are you currently planning to replace or upgrade your system(s)? (Please mark Y for yes and N for no and, if available, describe why, when and any estimated costs below)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

17. Do you publicize the intrusion detection system(s) you utilize? (Please mark Y for yes and N for no. If yes, explain how below)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

18. Do you currently track ongoing technology development in the area of intrusion detection? (Please mark Y for yes and N for no)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

19. Are investments in this area given a high priority in your transit system? (Please mark Y for yes and N for no)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

20. Have you identified intrusion detection needs for which there are currently inadequate products/systems to address them? (Please check and describe below)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

21. What is the extent of detection intrusion utilized at your system? (Please provide numbers and dimensions where appropriate)

	VIDEO SURVEILLANCE	ACCESS CONTROL	SENSORS	ALARM SYSTEMS	FENCES	BARRIERS	LIGHTING	HUMAN RESOURCES	OTHER
ADMINISTRATIVE BUILDINGS									
MAINTENANCE FACILITIES									
STORAGE FACILITIES									
RAIL YARDS									
OPERATIONAL CONTROL CTRS.									
POWER STATIONS									
TRAIN CONTROL SYSTEMS									
STATIONS									
TUNNELS									
BRIDGES									
TERMINALS & TRANSFER CTRS.									
RIGHT OF WAY									
PARKING LOTS & STRUCTURES									
TRAINS & RAIL VEHICLES									
BUSES									
SERVICE/SUPPORT VEHICLES									
SPECIAL PURPOSE VEHICLES									
PARA-TRANSIT VEHICLES									
ADDITIONAL INFORMATION (PLEASE SPECIFY):									

E. STATE OF THE PRACTICE (RESULTS OF SURVEYS, INTERVIEWS AND SITE VISITS)

1. State of the Practice - Tunnels, Bridges, and Right-Of-Way

Intrusion Detection Applications

There are portions of transit systems that are not intended for public access. Except in cases of station evacuation, tunnels, bridges, and right-of-way are restricted to authorized personnel only. Initially, access was controlled with the use of locked gates, fences, barriers, doors, and human resources. With the advent of technology, IDS and ACS electronic intrusion detection applications utilizing alarms, sensors, video surveillance and access control were installed in transit systems to detect and prevent access of non-authorized personnel to these restricted areas. Systems presently installed in these restricted areas are intended to enhance safety; reduce hazards, vandalism, and crime; and raise passenger perceptions about levels of safety and security within the transit system.

Transit agencies currently use many different types of systems. Tunnels and bridges use camera surveillance, access control, sensors, alarm systems, fences, barriers, lighting, and human resources. Transit agencies use fences, barriers, lighting, human resources, sensors, access control, and alarm systems to safeguard right-of-way.

All of the systems used are designed for safety and security, but some serve multiple purposes. IDS in tunnels, bridges, and right-of-way also serve an operating purpose, including the prevention of service delays that occur when an intruder or unauthorized personnel are present. Different types of sensors can also be used to detect hazards in the right-of-way that can be corrected without disruptions and delays in service. Other systems such as lighting, fencing, human resources, alarms, and communication systems, also contribute to a safe and efficient operation.

Many systems are used for preventive purposes, but some were installed in response to a specific incident. Depending on the factors that determine the type and mix of systems used, technology devices are frequently augmented with fences, barriers, or human resources.

Transit System Experiences

Based on survey results, the intrusion detection systems presently used in transit system tunnels, bridges, and right-of-way are generally functioning as intended and are viewed as having satisfied their original design purpose of reducing trespassing incidents. The exceptions occurred where access control systems did not prevent unauthorized access and vandalism within tunnels and right-of-way.

Although transit systems are generally satisfied with the performance of the intrusion detection systems, they have cited problems with false and nuisance alarms and camera reliability. Responding to intrusions is costly in terms of personnel and passenger inconvenience due to service delays. Improvements to fences and barriers alone do not discourage vandals from entering tunnels, bridges, and right-of-way, so electronic sensors and video surveillance are the applications usually considered in this area. Regardless of the problems experienced, most systems indicate that they would select the same application or product with technology upgrades that incorporate increased and improved functionality.

Failure rates for the intrusion detection systems utilized by transit agencies in tunnels, bridges, and right-of-way are fairly low, and most systems are considered to be quite reliable. Maintenance required for fences and barriers is quite low. Access control, alarm systems, and human resources require a moderate amount of maintenance, and video surveillance, sensors, and lighting require a higher amount of maintenance.

In addition to serving their initial purpose, a few secondary benefits of IDS have been achieved by transit systems. Secondary benefits have been noted through the use of access control, fences, barriers, and lighting at tunnels and through the use of human resources at tunnels and right-of-way. For example, human resources located at right-of-way may provide passengers with transit information as well as additional comfort and feelings of security.

The intrusion detection systems generally have not resulted in adverse effects on operations. The only adverse effects noted for these facilities are created by sensors and alarm systems in tunnels. These sensors occasional report false alarms that can result in service delays and employee time needed to respond to and verify alarms.

Transit agencies are using both customized and commercial off-the-shelf (COTS) products for intrusion detection systems in tunnels, and primarily COTS products for bridges. Agencies generally choose more customized products for right-of-way. Frequently, a COTS product or application may be used with minor modifications to operate to the agency's standards and requirements. This reduces the higher cost typically associated with purely customized applications.

Life expectancy for IDS in tunnels, bridges, and right-of-way varies based on the system and application selected. The life expectancy for video surveillance in both tunnels and bridges is 5 to 10 years. The life expectancy for access control systems, alarm systems, fences, barriers, and lighting when used in tunnels, bridges, and right-of-way is about 20 years. The life expectancy for tunnel sensors is 5 years.

As technology changes and evolves (particularly with video surveillance, electronic sensors, and access control), improvements are being made to systems for tunnels, bridges, and right-of-way. Following the review of security protocol after September 11, transit agencies have generally determined that the existing intrusion detection measures in tunnels, bridges, and right-of-way are adequate with some selected modifications to tunnel security components. While intrusions cannot be completely eliminated, additional protection can be provided. Security in tunnels has been supplemented with additional sensors, cameras, barriers, and human resources. Fencing and lighting have been repaired and enhanced where needed to diminish vandalism, and access control has been updated. It is important to note that intrusion detection systems in tunnels, bridges, and right-of-way are usually not publicized by transit agencies, with the exception of signs advising of video surveillance.

Future Needs

Technology development of the intrusion detection systems for tunnels, bridges, and right-of-way utilizing video surveillance, access control, sensors, and alarm systems are being closely tracked by transit agencies. Other applications do not require such careful tracking due to slower change cycles for products.

The investments for intrusion detection systems for tunnels, bridges and right-of-way are given high priority by transit professionals. These are crucial components of infrastructure, and protecting them is considered very important.

While receiving fairly high marks for reliability and service, the intrusion detection systems have certain limitations. For example, standard video surveillance does not operate well in dusty, poorly lit environments like tunnels. Improved technology should be investigated to deal with these circumstances.

2. State of the Practice - Stations, Terminals/Transfer Facilities, and Parking Lots/Structures

Intrusion Detection Applications

Stations, terminals (or transfer centers), and parking lots (or parking structures) are important customer and operating facilities for a successful transit system. These facilities provide the interface for passengers to connect with the transit system. By their very nature they must be open and accessible so the connection to buses or trains is seamless and convenient. While these facilities need to be open and easily accessible, they also require effective access control that accommodates fare collection and a safe movement of large numbers of people interacting with trains and buses. The open nature of these facilities poses unique challenges for protecting them from intruders.

Currently, transit systems use a mix of the following intrusion detection systems: video surveillance, access control, sensors, alarm systems, fences, barriers, lighting, and human resources are all designed to work together to provide intrusion detection and access control in transit system stations.

Terminals/transfer facilities utilize low-technology applications such as fences, barriers, lighting, and human resources to keep intruders out of areas designed for authorized personnel. As technology has evolved, these facilities have been equipped with video surveillance, access control, and alarm systems to improve detection and minimize the need for human resources.

Parking lots and structures are also protected with walls, fences, barriers, lighting, human resources, employee ID cards, and visitor passes. Technological advances added video surveillance, access control, and alarm systems.

Most of the IDS installed in transit stations were installed for preventive purposes, but video surveillance, alarm systems, and barriers in particular were positioned in response to a specific incident. Additional barriers were placed at terminals/transfer centers in response to an incident. Transit systems added alarm systems and barriers to their parking lots/structures in response to incidents.

Transit System Experiences

The IDS presently in use in transit system stations, terminals, and parking lots are generally functioning as intended and are viewed as having satisfied their originally designed purpose. Occasional vandalism still occurs at stations despite access control measures and video surveillance. Also, barriers and human resources are unable to prevent occasional thefts within parking lots and structures.

Failure rates for the intrusion detection systems utilized by transit agencies in terminals and parking facilities are fairly low, and most systems are considered to be quite reliable. The reliability of video surveillance can be low to moderate, but it may depend on the particular system used. Maintenance required for fences and barriers in stations is low. Access control, alarm systems, and human resources require a moderate amount of maintenance, and video surveillance, sensors, and lighting require a high amount of maintenance. As with stations, maintenance required for fences, barriers, and lighting. Access control, alarm systems, and human resources require a moderate amount of maintenance, and video surveillance, and human resources may require a high amount of maintenance.

Transit agencies indicate that they would usually select the same application or product if installing intrusion detection in stations again. On the contrary, transit agencies will not always select the same application or product when installing additional intrusion detection devices in terminals and parking facilities.

In addition to serving their initial purpose, a few secondary benefits have been achieved with IDS in stations, terminals and parking facilities. IDS at stations can be used for crowd monitoring and control, as well as reducing criminal activity. Human resources at stations, terminals, and parking lots can be a deterrent to criminal activity and provide customers with a higher sense of security. Additionally, human resources provide a resource for customer information on headways, routes, schedules, transfer points, landmarks, and fare media, thereby reducing the number of staff the transit agency must assign to each station.

The IDS generally have not resulted in adverse effects on operations. There have been occasional false and nuisance alarms at stations that can result in service delays and employee time devoted to responding to the problem. No adverse effects directly related to the intrusion detection systems were found in terminals and parking facilities.

Transit agencies use both customized and commercial off-the-shelf (COTS) products for their IDS. Fences, barriers, lighting, and alarm systems at stations are usually COTS, while video surveillance, access control, sensors, and human resources are composed of a mix of customized and COTS components. Agencies generally choose COTS products for lighting, employee IDsand visitor passes at terminals and parking lots.

The life expectancy for IDS applications in stations, terminals, and parking facilities generally conform to the ranges previously described, depending on the type and complexity of the system and the environmental installation conditions. To reiterate, fences, barriers and lighting have a life expectancy of 20+ years. Access control systems and simple alarm systems can expect to last for 10 to 15 years. Advanced sensors and video systems typically have a life expectancy of 5 to 7 years.

Replacements and upgrades planned for intrusion detection systems for stations and terminals will occur mostly with video surveillance and access control. These may not be upgraded at parking lots in the near future, however. Some transit agencies may also choose to update their human resources and lighting within stations as well.

Modifications have been made to the intrusion detection systems in stations to address the communications between incidents and response. Based on the type of incident, the first responder could be supervisors, police, emergency medical services or fire department personnel. Most systems within stations have been modified since inception. Modifications have been made to video surveillance, access control, lighting, and human resources in terminals. Modifications in parking facilities include video surveillance, access control, alarm systems, fences, barriers, lighting, human resources, and employee ID cards, and visitor passes.

IDS in stations, terminals, and parking facilities are not usually publicized by transit agencies. Exceptions occur for video surveillance in stations and parking facilities that provide the public with a degree of comfort in the event of an emergency and are physically noticeable by riders.

Future Needs

Technology development of the systems utilizing video surveillance, access control, sensors, and alarm systems for stations, terminals, and parking lots are being closely tracked by transit agencies. Other applications do not require such careful tracking due to slower change cycles for products. Emerging technologies may help to address current limitations of systems, such as that of video surveillance in conditions found in terminals and parking lots.

The investments for intrusion detection devices are given high priority by transit professionals, though sensors in both terminals and parking facilities are not considered a high priority. Sensors and alarm systems in stations may also be given a slightly lower priority than other IDS due to the high rate of false and nuisance alarms.

3. State of the Practice - Maintenance Facilities, Storage Facilities, and Rail Yards

Intrusion Detection Applications

Maintenance facilities, storage facilities, and rail yards are critical for the safe, efficient and successful operation of a transit system. Transit personnel staff these facilities and typically only employees and authorized visitors are granted access.

Maintenance, storage, and rail yards are equipped with most of the systems studied. They use video surveillance, access control, sensors, alarm systems, fences, barriers, lighting, and human resources. Additionally, maintenance facilities and rail yards use employee ID cards and visitor passes for additional security measures.

All of the IDS applications also serve an operating requirement in these facilities. While most systems were installed for prevention, alarm systems, video surveillance, barriers, and new access control

systems were installed in response to an incident. In most cases the incident was not specific to the transit agency; but was rather in response to the terrorist attacks of September 11, 2001.

Transit System Experiences

The intrusion detection systems presently used for these facilities function as originally intended, with a few exceptions. Access control has not been able to stop internal thefts at maintenance facilities and fences and lighting has not deterred occasional vandalism at maintenance facilities and rail yards. Video surveillance and access control do not always accomplish their intended purposes.

Failure rates for the intrusion detection systems utilized by transit agencies at maintenance, storage, and rail yard facilities are typically fairly low, and most systems are considered to be quite reliable. A few exceptions occur with video surveillance and access control. Moderate reliability was found with alarm systems, barriers, and human resources. Low levels of maintenance are required on most IDS for these facilities. Sensors and alarm systems require moderate levels of maintenance, while lighting and video surveillance sometimes require a higher level of maintenance.

If transit agencies were in the position of choosing systems for maintenance, storage, and rail yard facilities today, they would not necessarily choose the same product as they did initially. Access control, sensors, alarm systems, video surveillance and lighting products have changed and improved with new technology development.

Secondary benefits have been realized with most of the IDS at maintenance, storage, and rail yard facilities. These secondary benefits were not typically realized with the use of barriers, employee ID cards, and visitor passes at the facilities.

The IDS at these facilities generally have not had adverse effects on operations. While sensors and alarm systems designed for other components of a transit system have experienced false alarms, the only IDS that adversely affected these facilities were access control at maintenance facilities and alarm systems at rail yards. Maintenance, storage, and rail yard facilities mainly use commercial off-the-shelf (COTS) products for their IDS. These are sometimes modified to provide customized products used for access control, fences, barriers, video surveillance, lighting, and human resources.

The life expectancy for the IDS at maintenance, storage, and rail yard facilities are again similar to what has been previously described. Fences, barriers and lighting have a life expectancy of 20+ years. Access control systems and simple alarm systems can expect to last for 10 to 15 years. Advanced sensors and video systems typically have a life expectancy of 5 to 7 years. Transit agencies must plan for upgrades and replacement of all systems, particularly those high technology systems with shorter life expectancy.

Replacements and upgrades for IDS at these facilities are expected for some places in all categories. These decisions are based on the age and condition of the IDS that are currently operating.

The only systems publicized by transit agencies at maintenance, storage, and rail yard facilities are access control at maintenance facilities, employee ID cards, and visitor passes. All other systems are not publicized.

Future Needs

All of the systems for maintenance, storage, and rail yard facilities are tracked for ongoing technology development by some transit agencies.

Some transit agencies do not consider investments in sensors, alarm systems, fences, and lighting a high priority at these three facilities. They do consider video surveillance, access control, barriers, human resources, employee ID cards, and visitor passes high priority investments.

Several of the systems used at maintenance, storage, and rail yard facilities do not address all current needs. These systems include video surveillance, access control, sensors, and alarm systems. Transit agencies must consider these needs with upcoming plans for replacement and upgrades of current IDS/ACS.

4. State of the Practice - Power Stations, Train Control Areas, and Operational Control Centers

Intrusion Detection Applications

Power stations, train control areas, and operational control centers are highly technical facilities required for the effective operation of a transit system. They are usually located separately from other transit functions, and require fewer employees per square foot of space. Operational control centers serve to monitor, coordinate and direct the operations of both trains and buses consistent with schedules and the operating and safety standards of the transit agency. Power stations and train control areas are associated with electrified rail transit operations. Power stations regulate the electricity necessary to operate rail vehicles and train control areas house the sophisticated equipment that operates the computerized signal, automated train control and communications systems for the entire rail system. All of these facilities are restricted to authorized personnel only. Unwanted intrusion into any of these facilities jeopardizes the very heart of the transit operation. As a result, special efforts for intrusion detection and strict access control exist at each of these facilities.

These facilities are commonly equipped with systems including access control, alarm systems, fences, lighting, video surveillance, sensors, barriers and human resources. Of these devices, access control installed in operational control centers and train control systems serve an operating requirement in addition to security functions. This is also the case for sensors and alarm systems at power stations and train control areas, lighting at operational control centers and power stations, and human resources at operational control centers and train control systems. While these have been primarily installed for prevention, barriers are often added at operational control centers and power stations in response to a specific incident.

Transit System Experiences

Typically the IDS presently used function as originally intended, with the exception of video surveillance at operational control centers. Other IDS devices at power stations and train control systems operate to design. Failure rates for the IDS utilized by transit agencies at power stations, train control areas, and operational control centers are fairly low, and most systems are considered to be quite reliable. Maintenance varies based on the type of intrusion detection device. Some video surveillance products used in power stations, train control centers, and operational control centers

require very little maintenance while other products require a high amount of maintenance. Unreliable cameras (failure rates up to 75 percent) are being replaced slowly. Access control, alarm systems, fences, and barriers require a moderate amount of maintenance, and lighting varies on the amount needed for full performance

Transit agencies would not necessarily select the same products if making the same decision again for power stations, train control areas, and operational control centers. Video surveillance, access control, alarm system, and lighting are the areas in which new technology has been developed and transit agencies indicated they would choose the newer, more technologically advanced product, if making the decision today.

Secondary benefits have been achieved at all three facilities through the use of access control, alarm systems, fences, and lighting. Additionally, secondary benefits have been noted at operational control centers with video surveillance, barriers, and human resources. If an employee has been terminated, the access control system provides a method to immediately remove the former employee's ability to access the building (and potentially to the operations controls center of the transit system).

IDS systems generally have not had adverse effects on operations at power stations, train control areas, and operational control centers. Occasionally false and nuisance alarms are reported at train control areas, but the other IDS for these three facility types have caused no adverse effects.

Operational control centers are somewhat unique facilities with regard to the origin of their IDS products. IDS found at operational control centers are usually commercial off-the-shelf (COTS) products. Modifications have been made to video surveillance and access control products to configure the resource to the particular needs and requirements of the transit agency. The products utilized at power stations and train control systems are also usually COTS products, with custom configuration of access control at both facilities, alarm systems at train control systems, and fences and barriers at power stations.

Life expectancy for intrusion detection systems at power stations, train control systems, and operational control centers is consistent with that of IDS for other facilities. Fences, barriers and lighting have a life expectancy of 20+ years. Access control systems and simple alarm systems can expect to last for 10 to 15 years. Advanced sensors and video systems typically have a life expectancy of 5 to 7 years. Upgrades planned for these facilities will utilize rapidly changing technology in the areas of video surveillance, access control, and alarm systems. Upgrades to existing sensor technology at train control systems is expected, as well as upgrades to fences at power stations and operational control centers and barriers at power stations.

Since the systems were installed at power stations, train control areas, and operational control centers, several modifications have been made. These modifications have occurred with access control, alarm systems, fences, and barriers. Additionally, operational control centers have experienced modifications to video surveillance and human resources, while train control areas have upgraded sensors. Visitor procedures have also been reviewed and revamped.

Access control is the only systems publicized by transit agencies at operational control centers. All other IDS (including all IDS at power stations and train control areas) are not publicized.

Future Needs

In addition to the standard technology development monitoring of video surveillance, access control, sensors, and alarm systems, fences and lighting are also being monitored with respect to technology changes and how they can improve systems at power stations, train control areas, and operational control centers. Transit agencies tend to consider investments in video surveillance, access control, alarm systems, sensors, fences, barriers, lighting, and human resources a high priority.

Although intrusion detection systems typically have limitations, there are only two IDS applications that seem to need improvement. These are video surveillance at operational control centers and alarm systems at power stations.

5. State of the Practice - Administrative Facilities

Intrusion Detection Applications

Administrative buildings house many employees of a transit agency, and in many instances are located close to (and in some cases integral to) a transit stop, terminal, or station. These buildings usually house the senior executives of the agency and most of the administrative support staff. Administrative buildings also experience a large volume of visitors. Customers, visitors, suppliers, job applicants, media and the general public can seek access to administrative buildings on any given day. Sensitive information is often located in such buildings, and agencies have an obligation to protect the building, its contents and employees from unauthorized intruders.

Currently, several systems applications are used at most administrative buildings. These include video surveillance, access control, sensors, alarm systems, fences, barriers, lighting, and human resources. While they all enhance security, access control, alarm systems, lighting, and human resources also meet an operating requirement for some transit agencies.

In many instances barriers and improved access control systems were added to administrative building security in response to a specific incident. Additional IDS were installed for preventive purposes.

Transit System Experiences

The IDS used by transit systems in administrative facilities are typically functioning as originally intended and accomplishing intended purposes. Exceptions occur with video surveillance and access control systems. Contributing to the success of the IDS is the reliability of the systems chosen. Most of the components used for administrative facilities are quite reliable, although higher failure rates may be found with the technology devices - video surveillance systems, access control systems, sensing devices, and alarm systems.

Maintenance on administrative building systems varies greatly depending on the product chosen. Video surveillance, sensors, alarm systems, and lighting usually require a high amount of maintenance, while access control, fences, and barriers usually require very little. Exceptions of course occur, with some transit agencies reporting that their video surveillance, sensors, and alarm

systems require very little maintenance. The particular product chosen usually determines the reliability and maintenance required.

Transit systems would typically choose the same product again, despite some problems with maintenance and reliability. The IDS transit agencies might not choose again typically involve varying technological products.

Transit systems indicated that secondary benefits have been achieved through the IDS selected for their administrative facilities. These benefits were of the types discussed in the introduction.

Adverse effects on transit operations have occurred with access control and sensor systems at administrative facilities. These occurrences have included false alarms and additional personnel to monitor alarms.

Transit systems are using a combination of customized and commercial off-the-shelf (COTS) products for all the systems used at administrative buildings. Customized systems occur more frequently in applications using video surveillance, access control, sensors and alarms.

As described in the introduction, life expectancy of IDS applications at administrative buildings depends on the component chosen. Fences, barriers, and lighting have the standard life expectancy of more than 25 years. Transit systems reported that their access control systems and simple alarm systems have a life expectancy of 10 to 20 years, while more complex alarm systems, video surveillance systems, and sensors have a life expectancy of only about 5 to 10 years. Upgrades are planned for video surveillance, access control, sensors, and barrier systems at some administrative buildings.

Modifications have been made to nearly all IDS at administrative buildings since their initial installation. In most instances the modifications involved upgrades of the technological components. General strengthening of the systems components have occurred since the security protocol review following September 11, 2001.

As mentioned in the Introduction, information on costs was collected from vendor and manufacturer sources. That information is provided in other sections of this report.

The only intrusion detection application publicized at administrative buildings is access control.

Future Needs

Technology development is tracked by some transit agencies for all of the IDS used at administrative buildings. Typically, investments in all the areas of IDS and ACS used at administrative facilities are given a high priority.

The needs that are not currently being met at administrative buildings occur with the IDS of video surveillance, sensors, and alarm systems.

Abbreviations used without definitions in TRB publications:

AASHO	American Association of State Highway Officials
AASHTO	American Association of State Highway and Transportation Officials
APTA	American Public Transportation Association
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
ATA	American Trucking Associations
CTAA	Community Transportation Association of America
CTBSSP	Commercial Truck and Bus Safety Synthesis Program
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FMCSA	Federal Motor Carrier Safety Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
IEEE	Institute of Electrical and Electronics Engineers
ITE	Institute of Transportation Engineers
NCHRP	National Cooperative Highway Research Program
NCTRP	National Cooperative Transit Research and Development Program
NHTSA	National Highway Traffic Safety Administration
NTSB	National Transportation Safety Board
SAE	Society of Automotive Engineers
TCRP	Transit Cooperative Research Program
TRB	Transportation Research Board
U.S.DOT	United States Department of Transportation